

August 26, 2024

VIA ELECTRONIC MAIL:

Dear \_\_\_\_\_ :

**Re: Request for Access to Records – Response**  
***Freedom of Information and Protection of Privacy Act (FOIPPA)***

I am writing further regarding your request received by the BC Energy Regulator (BCER) for the following records:

- **Acceptable use of technology policy instruments (where “instrument” has the same meaning as in Treasury Board Directive 1/23) and onboarding materials.**
- **File plans/lists/indexes and/or records management ontologies/thesauri.**
- **Public body self-assessments and audits/evaluations of records/information management.**
- **Policy instruments regarding records of information management.**
- **Copies of records retention schedules.**
- **The public body’s information resources/information asset/record management plans, as applicable; and,**
- **Licenses, contracts, or agreements between the public body and recordkeeping system service providers or contractors.**

**Date range: 1 January 2021 to 16 July 2024**

Please find attached the records located in response to your request. Some information has been withheld pursuant to section(s): *13 (Policy advice or recommendations) and 17 (Disclosure harmful to the financial or economic interests of a public body)*. A complete copy of FOIPPA is available online at: [Freedom of Information and Protection of Privacy Act \(gov.bc.ca\)](https://www.gov.bc.ca/foi-proactive-disclosure-policy). Please note, copies of records retention schedules were included in the response for Request BCER2024-001 provided to you on July 10<sup>th</sup>.

A copy of these records will be published on the BCER’s website within five business days after release. To find out more about proactive disclosure of requests, please access the BCER website: [foi-proactive-disclosure-policy.pdf \(bc-er.ca\)](https://www.bc-er.ca/foi-proactive-disclosure-policy.pdf). Your file is now closed.

Pursuant to section 52 of the FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review any decision, act, or failure to act with regard to your request under FOIPPA within 30 business days by writing to:

*Information and Privacy Commissioner  
PO Box 9038 Stn Prov Govt  
4<sup>th</sup> Floor, 947 Fort Street  
Victoria BC V8W 9A4  
Phone: 250.387.5629 Fax: 250.387.1696  
Email: [info@oipc.bc.ca](mailto:info@oipc.bc.ca)*

If you request a review, please provide the OIPC with a copy of your original request, a copy of the BCER's response, and the reasons or grounds upon which you are requesting the review. Further information on the complaint and review process can be found on the OIPC website: <https://www.oipc.bc.ca>. Please write [FOIIntake@bc-er.ca](mailto:FOIIntake@bc-er.ca), if you have any questions regarding your request or require any further clarification.

Sincerely,

*D. Keough*  
BC Energy Regulator



## INFORMATION MANAGEMENT IN ONEDRIVE

### Microsoft OneDrive

Microsoft (MS) OneDrive is a cloud based personal workspace provided to each Microsoft 365 user for information and materials related to their work. Records within OneDrive can only be accessed by the user, unless they specifically grant permission to share a document with another person(s).

*As OneDrive implementation evolves, guidance will be updated.*

### Recordkeeping roles and responsibilities

To comply with the *Information Management Act*, the Commission must retain all official records in an appropriate recordkeeping system.

OneDrive is not an appropriate repository for long-term storage of Commission records: information is not accessible to others who may need it (e.g. when an employee is absent); and information is not easily searchable for FOI or legal requests. Keeping information in OneDrive creates information silos.

It is intended for short-term storage of records being actively worked on, i.e. drafting a new document, or personal reference material.

Employees are responsible for ensuring critical information that they create or receive is filed in an appropriate recordkeeping system (most often, within folders on our shared drives).

**Critical Records** include official or final copies, substantial drafts, correspondence, and other records that document decisions and actions.

### Documenting Commission Decisions

If records in OneDrive contain important decisions, or context for those decisions, they must be retained. For more information on the requirements to document decisions, see the [Documenting Commission Decisions](#) resource material.

### Freedom of Information and Protection of Privacy roles and responsibilities

Information in OneDrive is subject to requests under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

#### **Freedom of Information (FOI):**

Employees are responsible for information searches in response to FOIPPA requests and other legal obligations within their OneDrive.

#### **Protection of**

**Privacy/Confidentiality:** Although it is a personal workspace, OneDrive supports collaboration through the ability to share OneDrive documents through Teams or emails. When sharing a document, care must be taken to ensure sensitive or confidential material is only viewed by those who need to see it.

Limit sharing sensitive or confidential information (e.g. personal information), as you would with any communication tool; for example, when sharing a link in an email, check that only the appropriate people have access.



## WHAT MUST I DO WITH INFORMATION IN ONEDRIVE?

Each employee is responsible to ensure information is appropriately managed in the OneDrive environment.

### File critical information on OneDrive to a recordkeeping system, i.e. shared drives.

Because OneDrive is not an appropriate recordkeeping system, and critical information is to be filed elsewhere, OneDrive should only hold transitory information (i.e. information that is not required to meet legal obligations or to sustain administrative or operational functions). Transitory information may be deleted when no longer needed.

One Drive is similar to your F: drive as your individual storage space. This is a place to store information and documents that you are not ready to make official or share with your team yet, or that are for your personal use only. You are the only person with access to your OneDrive.

You can store personal copies of HR-type records, convenience copies of reference material, and drafts – until they are finalized, or ready to share with your team.

### Share documents carefully.

You are responsible for managing permissions to documents you store in your OneDrive. When you select permissions, you are choosing who will be able to access your document. Only give permission to individuals who need to access the information. There are a few ways to share documents in OneDrive; be sure to select the sharing method which is appropriate to the sensitivity of the document.

#### Best practice

Regularly review your OneDrive and routinely transfer any official records to your recordkeeping system. Delete any transitory information that is no longer needed.

Consult the [Official vs Transitory Records](#) guide to learn more about what you should move to a shared drive, and what you can delete.



# MANAGING INFORMATION IN SHAREPOINT

## Microsoft SharePoint

SharePoint is a document management and collaboration tool in Microsoft Office 365. It is used to collaborate and share content across an organization. It can also be used as a records management tool. This guide provides advice and guidance on using SharePoint to manage commission records.

Under the *Information Management Act (IMA)*, government bodies must ensure that an appropriate system is in place for creating and maintaining government information. If managed appropriately, SharePoint can be part of that system.

## Planning to implement SharePoint

Implementing a SharePoint site should involve the same careful planning as required for any system implementation. This generally includes the following steps:

- A. Requirements gathering and analysis
- B. Gaining and maintaining management commitment and support for the project
- C. Pre-implementation architecture, design, configuration and testing
- D. Establishing governance, user training, and communications protocols
- E. Post-implementation testing and monitoring
- F. Post-project document migration to a recordkeeping system and closing the SharePoint site

Assign responsibility for managing and filing records at the start. Do not wait until the site project/purpose is over before identifying who needs to manage and file the documents into the appropriate recordkeeping system.

SharePoint Site Owners are responsible for:

- Identifying appropriate site users and permissions.
- Creating and managing document Libraries and Content Types.
- Ensuring documents are migrated to a recordkeeping system at project completion or site closure.

**This guide only applies to the M365 SharePoint application.**

It does not apply to records and information in Teams.

Teams uses SharePoint for short-term collaboration. However, Teams is not an approved recordkeeping system under the IMA. Once you are finished collaborating on a document in Teams, it should be saved to your recordkeeping system.

Do not keep final document versions in Teams SharePoint for long-term storage



## Using SharePoint to manage your records

There are many ways to use and configure SharePoint. The following best practices provide some basic records management measures for the records maintained there:

- **Establish and document responsibility for the site and access to it. Keep that documentation up to date.** Site Owners need to ensure all access permissions are kept current. This enables authorized staff to locate the records and information they need for operational, FOI or other legal purposes.
- **Implement an ARCS and ORCS structure upfront.** SharePoint sites should be organized according to approved information schedules (ARCS/ORCS). This involves mapping site content to specific record classifications. Contact Records and Information Services for guidance on how to do this.
- **Document design and configuration decisions.**

Site Owners are responsible to ensure information is appropriately managed in the SharePoint environment.

- **Use naming conventions for documents.** Try to consistently title documents with established naming conventions, or using standard elements (e.g. a clear description of the document, version number, and creation date).
- **Delete transitory information regularly.** Information management rules apply to records in SharePoint. Transitory records may be routinely deleted by employees. All other records must follow the retention schedules outlined in ARCS/ORCS.

## FOI, Privacy and Confidentiality of Information

Information in SharePoint is subject to access requests under the *Freedom of Information and Protection of Privacy Act (FOIPPA)*.

When using SharePoint, ensure you:

- Are prepared to respond with copies of responsive records for FOI or other legal obligations.
- Limit sharing personal, sensitive or confidential information to only what is necessary for conducting Commission business.

### Shutting down your SharePoint site?

Contact Records and Information Services first.

Your records may need to be migrated to a recordkeeping system once the site is no longer in use.

We will help guide you on the best course of action.



# MANAGING INFORMATION IN TEAMS

## Microsoft Teams

Microsoft (MS) Teams is a communication and collaboration tool in Office 365. Features include one-on-one chats, team chats, document collaboration, video meetings, and integration with other shared applications. Each MS Team has a designated Team Owner.

*Page one in this guide identifies our legislated requirements and responsibilities in the Teams environment. Page two clarifies how we manage our information in Teams.*

## Recordkeeping Roles and Responsibilities in Teams

The Commission is governed by legislation and policy which requires us to create and keep adequate records of our decision-making and work activities.

Teams does not have the necessary functionality and controls for an appropriate recordkeeping system. It is a tool for communication and collaboration. When working in Teams:

**Employees** need to ensure critical information that they create in Teams is filed in an appropriate recordkeeping system (most often, this is our shared drives).

**Team Owners** are ultimately responsible for ensuring critical information within their Teams sites is filed in the recordkeeping system.

**Critical information** includes official or final copies, substantive drafts, correspondence, and other records that document decisions and actions.

You may have critical information in meeting recordings, chat messages, collaborative documents, or Planner tasks.

When documenting decisions made in Teams, remember to include the context for that decision (e.g. the discussion or chat thread that lead to the decision). For more information, see the [Documenting Commission Decisions](#) resource material.

## Freedom of Information and Protection of Privacy (FOIPPA) Roles and Responsibilities in Teams

### Freedom of Information (FOI):

As with all Commission records, information in Teams may be requested under FOIPPA. When working in Teams:

**Team Owners**, under the direction and guidance of the FOI team, are responsible for ensuring records searches are done in response to FOI requests and other legal obligations.

**Employees** should be prepared to respond to a records search request when notified by a Team Owner.

### Protection of Privacy/Confidentiality:

**Employees** should try to limit sharing personal, confidential or sensitive information, as you would with any communication tool. When sharing information in Teams, remember that Team membership may change over time and include external employees or contractors.



## WHAT MUST I DO WITH INFORMATION IN TEAMS?

*Team Owners are responsible to ensure information is appropriately managed in the Teams environment.*

### File critical information from MS Teams to a recordkeeping system:

Because Teams is not an appropriate recordkeeping system, Teams primarily holds transitory information (i.e. information that is not required to meet legal obligations or to sustain administrative or operational functions). Transitory information is eligible for deletion when no longer needed.

Everything you do in Teams should be for collaboration purposes only. This is not a place to store documents for future use or preservation purposes. Once you are finished collaborating on a document, it should be saved to your recordkeeping system (shared drive).

**Final versions of documents should not be kept in Teams for long term storage.**

### Manage chat messages:

Avoid using Team chats for conversation that will have operational/strategic value and must then be managed. If this happens, you must document these chat messages in a retainable format, such as a memo or email which can be stored on a shared drive:

- Copy, summarize, or transcribe the information to another document, and
- File it in your recordkeeping system.

### Understand chat retentions

It is important to understand how long your chat messages remain in Teams, so that you can save critical messages in time:

- Ad hoc chat messages outside Teams channels will be deleted in 10 days.
- Department/branch Teams chat messages will be deleted from Teams after 3 months.
- Project or committee Teams chat messages remain in Teams for the duration of the project.

### Save critical records from external Teams:

If you are part of a Team for an inter-jurisdictional committee, the host Team's retention rules govern the information shared in the Team space. Ensure critical records for the Commission's role in the committee are captured in the recordkeeping system.

#### Best Practice

Regularly review your Teams documents and chat channels, and copy out any information that is critical to your operations, or part of an official record.

Consult the [Official vs Transitory Records](#) guide to learn more about what you should move to a shared drive, and what you can leave in Teams as transitory information.



ISSUANCE: People, Reconciliation and Transformation Division  
Information Systems & Technology

APPROVED: June 14, 2023

## 1.0 GENERAL

### 1.1 Purpose

This policy is intended to guide employees in the suitable use of BC Energy Regulator (BCER) information and technology (IT) resources. Employees are required to sign off annually on the policy.

This policy has been developed to:

- Promote IT knowledge and appropriate resource usage throughout the organization.
- Maximize productivity and minimize risks to BCER network security and performance.
- Protect the privacy, confidentiality, and security of BCER information systems, technology, and information (e.g., data, documents, records, content, etc.).
- Improve adherence to government information and technology-related legislation, policies, and standards.
- Promote public trust in the BCER's use of information and technology assets.

Any questions regarding the interpretation or application of this policy should be directed to the Executive Director, Information Systems & Technology, or to the Director, Information Technology.

### 1.2 References

- [\*Employee Code of Conduct and Ethics Policy\*](#)
- [\*Information Security Policy\*](#)
- [\*BC Office of the Chief Information Officer Security Policy\*](#)
- [\*Government Core Policy and Procedure Manual section 12.3\*](#)
- [\*Freedom of Information and Protection of Privacy Act\*](#)
- [\*Mobile Device Policy\*](#)
- [\*Managing Confidential Information Guide\*](#)
- [\*Building Access and Security Policy\*](#)
- [\*Information Management Act\*](#)
- [\*Information Management Policy\*](#)
- [\*Interim Privacy Breach Notification Policy\*](#)

### 1.3 Application and Scope

Employees shall use IT resources in accordance with the Employee Code of Conduct and Ethics policy. As a condition of employment, employees are expected to take responsibility for, and accept the duty to, actively protect BCER information and technology assets. This includes being aware of, and adhering to, all relevant legislation, policies, and standards.

Improper use may jeopardize the confidentiality, integrity, and availability of BCER information and technology assets, and put personal and/or sensitive information, security, and service levels at risk.

## 2.0 POLICY

- 2.1 IT resources refers to BCER owned hardware and software, including but not limited to:
- Laptops, desktops, tablets
  - Mobile phones
  - Web conferencing
  - BCER email
  - Monitors, mice, keyboards, headsets
  - Docking stations
  - Data projectors, USB sticks
- 2.2 The purchase of hardware, software, and cloud services will be done through the Information Systems and Technology department and may require:
- The completion of a fair procurement process; and/or
  - A completed privacy impact assessment (PIA) and security threat and risk assessment (STRA).
- 2.3 Regarding the use of IT resources, employees have an obligation to not:
- Circumvent or subvert the BCER Information Security Policy, cybersecurity controls or procedures.
  - Leave BCER devices unattended and unlocked whether in the office or while working remotely.
  - Use non-BCER approved services (e.g., AI language models, private cloud storage, email, file transfer, etc.) or devices to send, receive or exchange information about the BCER.
  - Save BCER information on local hard drives of workstations, laptops, tablets, or mobile phones except as defined in Section 2.8.
  - Use IT resources in a manner that inappropriately discloses, shares or compromises BCER information.
  - Use natural language AI models with inputs with specific BCER information. Inputs must be genericized.
  - Use IT resources in a manner that violates Canadian or BC laws.
  - Use IT resources in a manner that negatively impacts or disrupts BCER business or operations.
  - Use IT resources to download non-work-related files (e.g., Freeware, Shareware, illegally obtained movies or music files); Stream video over BCER network resources, unless the access is work-related and authorized.
  - Install unauthorized applications on BCER devices.
  - Share BCER login credentials with others.
  - Record password(s) in a manner that could compromise security (e.g., on sticky notes left on monitors, inside desk drawers or under pen/pencil trays, etc.).
- 2.4 Any content created, received, or transmitted using BCER equipment or retained within the BCER's network will be appropriately managed as a BCER record in accordance with applicable legislation and policy.
- 2.5 There can be no expectation of personal privacy related to the use of BCER information technology resources except for specific privileged communications (i.e., Cabinet,

solicitor/client, and union representative communications).

- 2.6 Any collection, access, use and/or disclosure of Personal Information must be done in accordance with the *Freedom of Information and Protection of Privacy Act* and its supporting policies. This includes mandatory completion of a PIA to assess and mitigate risks.
- 2.7 If an information/privacy breach (i.e., unauthorized file access) or cybersecurity incident occurs, employees and supervisors must report to the BCER’s Cybersecurity team and designated Privacy Officer(s) without delay.
- 2.8 Only while employees are traveling or working remotely may work related documents be saved on a local hard drive temporarily. Priority when working remotely is to use GlobalProtect to access BCER files or systems. Local hard drive files should be deleted once in the office.
- 2.9 Employees must be cybersecurity aware. This includes completing mandatory training and practices such as using strong passwords, scrutinising email for phishing attacks and reporting suspicious links or files.

**3.0 LIMITED PERSONAL USE**

- 3.1 Employees are permitted limited personal use of BCER IT resources. Personal use of BCER IT resources should not occur during peak hours (i.e., 8 a.m. to 5 p.m. weekdays) and must be consistent with the Employee Code of Conduct and Ethics and Information Security policies.
- 3.2 Personal use of BCER pooled IT resources (during or outside of office hours) must be approved by the resource owner and scheduled through the Resource Scheduler.
- 3.3 Storage of personal pictures, music, or videos on an employee’s local workstation (C: drive), tablet or mobile phone is acceptable; however, they must not be stored on the network. IT does not back up these types of files.

**4.0 APPROVAL**

Approved by the Executive Team on June 14, 2023

**Version Control:**

Revision V1	Dec-13	Administrative Updates
Annual Review	Oct-14	No Changes
Annual Review	Oct-15	No Changes
Revision V2	Nov-16	Added Sections 2.3 - 2.5
Revision V3	Dec-17	Administrative Updates
Annual Review V4	Nov-18	No Changes
Annual Review V4	Apr-20	Administrative Updates (Title)
Revision V5	23-Jun	Updated Policy



BRITISH COLUMBIA ENERGY REGULATOR

# POLICY

<b>Policy Name</b>	Use of IT Resources Policy
<b>Policy Number</b>	UP1
<b>Approving Authority</b>	Executive
<b>Designated Executive Officer</b>	Sara Dickinson, Executive Vice President, People, Reconciliation & Transformation
<b>Effective Date</b>	August 06, 2024
<b>Last Reviewed</b>	June, 2024
<b>Next Review</b>	April, 2025

## 1.0 PURPOSE

The purpose of this policy is to ensure that BCER’s Information Technology (IT) resources, provided to employees to enhance their productivity, are used responsibly and ethically, and in compliance with BC Government legislation and BCER policies. This policy does not attempt to anticipate every situation that may arise and does not relieve anyone accessing any system of their obligation to exercise good judgment.

Any questions regarding the interpretation or application of this policy should be directed to one of the following:

- Executive Director, Information Systems & Technology.
- Director, Information Technology.
- Director, Information Security.

## 2.0 APPLICATION AND SCOPE

This policy applies to all IT Resources that are managed by the BCER, including computers, software, communication devices, network, and cloud-based devices and software.

Employees shall use IT Resources in accordance with the Employee Code of Conduct and Ethics policy. Employees are required to take responsibility for and actively protect BCER information and technology assets. This includes being aware of, and adhering to, all relevant legislation, policies, and standards.

Improper use may jeopardize the confidentiality, integrity, and availability of BCER information and technology assets, and put personal and/or sensitive information, security, and service levels at risk.

### 3.0 DEFINITIONS

- A. **IT Resources:** Refers to the technology, information/data assets provided by the organization to its employees to enhance their productivity, including but not limited to:
- Laptops, desktops, tablets.
  - IT peripherals such as monitors, mice, keyboards, headsets, docking stations.
  - Corporate Property issued mobile phones.
  - Storage media such as USB sticks, hard drives.
  - Data (such as BCER email, network files).
  - Software and cloud services such as M365 (Teams, Word, Excel, PowerPoint, One Drive).
  - Other devices with a network connection or requiring software.
- B. **Large Language Models:** A type of artificial intelligence algorithm that uses deep learning techniques and massively large data sets to understand, summarize, generate, and predict new content.

### 4.0 POLICY REQUIREMENTS

- A. Employees must not access and/or purchase technology, devices, applications, or services (known as “shadow IT”) that are not authorized and approved by Information Systems & Technology (IST). Purchases must include a fair procurement process and the completion of a Privacy Impact Assessment (PIA) and Security Threat and Risk Assessment (STRA).
- B. The use of Artificial Intelligence (AI), including Large Language Models, within the BCER must follow principles of ethical conduct, transparency, and accountability.
- C. IT Resources and BCER issued accounts must be used only by the employee to whom they have been assigned.

- D. Employees must always protect all corporate-managed IT Resources, ensuring they are physically and logically secured and remain under the employee's control. IT Resources must not be left unattended and/or unlocked, whether in the office or while working remotely.
- E. All content created, received, transmitted, or retained for BCER business purposes must be appropriately managed as a BCER record in accordance with applicable legislation and policy.
- F. BCER documents and information must only be stored within BCER managed systems. Work-related documents may only be copied to a local hard drive while employees are offline, however, they must be copied back to BCER managed systems as soon as the employee returns from the remote location.
- G. BCER employees have limited personal privacy when using business resources. Business resources may be subject to collection of information for freedom of information requests, security investigations, or other purposes.
- H. The collection, access, use and/or disclosure of Personal Information must be done in accordance with the Freedom of Information and Protection of Privacy Act. Any new or revised collection, access, use and/or disclosure of Personal Information must first be approved via the BCER Privacy Impact Assessment process to ensure identification, assessment, and mitigation of risks.
- I. Information/privacy breaches (e.g. unauthorized file access) or cybersecurity incidents must be reported to the BCER's Cybersecurity team and designated Privacy Officer(s) without delay.
- J. A strong cybersecurity posture is the collective responsibility of all BCER employees. Active participation in cybersecurity training sessions and adherence to best practices (such as creating and maintaining strong passwords, exercising vigilance in identifying and reporting phishing attempts, and promptly reporting any suspicious activity) is mandatory. Employees must not circumvent or subvert the BCER Information Security Policy, cybersecurity controls or procedures.
- K. Good IT Resource hygiene must be practiced. This includes following IST instructions, notifications, and device maintenance prompts to ensure systems are secure, reliable, and up to date with features and functionality.
- L. Employees are permitted limited personal use of BCER IT Resources if personal use of BCER IT Resources does not impact business operations and is consistent with the Employee Code of Conduct and Ethics, Information Security Policy, Canadian law, and British Columbia laws.

## **5.0 RELATED LEGISLATIVE REFERENCES**

- [Freedom of Information and Protection of Privacy Act](#)
- [Information Management Act](#)

## **6.0 RELATED BCER POLICIES**

- [Employee Code of Conduct and Ethics Policy](#)
- [Information Security Policy](#)
- [Mobile Device Policy](#)
- [Managing Confidential Information Guide](#)
- [Building Access and Security Policy](#)
- [Information Management Policy](#)
- [Procurement policy](#)

## **7.0 AUTHORITIES AND OFFICERS**

- a) Approving Authority – Executive
- b) Designated Executive Officer – Sara Dickinson, Executive Vice President, People, Reconciliation & Transformation
- c) Procedural Authority – Executive
- d) Procedural Officer – Ab Dosil, Executive Director, Information Systems & Technology

INFORMATION LOCATIONS IN THE COMMISSION							
Record type	Record locations			Contact	Program area	FOI notes	Notes
	electronic	paper	system				
Land use planning review	K: drive / outlook			Sean Curry	Operational Policy & Environment		
Corporate Registry / company files			KERMIT	Shannon Weatherill / Jody	Permitting		FSJ base for this function
Name changes / amalgamations /	K: drive	offsite	TANC	Shannon Weatherill / Jody	Permitting		
Board of Director records	K: drive / outlook	offsite		Stacey Bligh	Board Services		
Archaeology				Vera Brandzin	Heritage Conservation		
Archeaology permits	K: drive	FSJ File Room		Vera Brandzin	Heritage Conservation		FSJ base for this function
Archeaology non-compliance files	K: drive	FSJ File Room		Vera Brandzin	Heritage Conservation		FSJ base for this function
Archeaology audits	K: drive	FSJ File Room		Vera Brandzin	Heritage Conservation		FSJ base for this function
Indigenous relations - strategic	K: drive	offsite		Kelly Wintemute	Strategic Engagement		Prince George base for
Indigenous consultation - applications	K: drive	Application file in FSJ File Room (pre-2016)	AMS since 2016	Adam Kamp / Ryan Stark	Permit Adjudication / Decision Support		FSJ base for this function
Indigenous agreements	K: drive	?		Kelly Wintemute	Strategic Engagement		
Indigenous awareness and training	K: drive			Kelly Wintemute	Strategic Engagement		
Applications (for activity permits)		Application file in FSJ File Room (pre-2016)	AMS since 2016	Shannon Weatherill / Jody Sutherland	Permitting		Including well, geothermal (since 2018), pipeline, facility, LNG facility, road, geophysical permits and all associated oil and gas
Applications for EMA activities		EMA files in FSJ file room		Rachel Butler	Operational Policy & Environment		
Applications for ARCH activities		ARCH files in FSJ file room		Vera Brandzin	Heritage Conservation		
Geothermal wells	K: drive	Kelowna offices (?)	"IRIS mirror system"	Jordan ven Besouw	Drilling Engineering & Technical Services		
Application review - Indigenous consultation working files				Adam Kamp / Ryan Stark	Permit Adjudication / Decision Support		
Application review - LNG projects	K: drive (notes?)	Application file in FSJ File Room (pre-2016)	FTP site, AMS for final notes (since	Suzanne Matthews	Drilling Engineering & Technical Services		
Application review - Archaeological	K: drive (notes?)	Application file in FSJ File Room (pre-2016)	AMS for final notes (since 2016)	Vera Brandzin	Heritage Conservation Program		



Application review - Engineering	K: drive (notes?)	Application file in FSJ File Room (pre-2016)	AMS for final notes (since 2016)	Kevin Parsonage	Engineering, Integrity & Technical Compliance		
Application review - Geological Complaints	K: drive		AMS for final notes KERMIT	Jeff Johnson	Petroleum Geology		
Enforcement investigation cases	K: drive				C&E		
Inspections - compliance	K: drive (still?)		KERMIT		C&E		
Contravention decisions	K: drive			Andy Johnson	C&E		
Orders: compliance	K: drive			Andy Johnson	C&E		
Orders: s. 75	K: drive			Ron Stefik	Reservoir Engineering		Reservoir engineering
Orders: securities (s. 30)	K: drive			Wade Abbott / Mike Janzen	Liability Management		Orphan and Liability
Orders: s. 38							
Integrity Management Program - external audit	K: drive	Kelowna offices		Gouri Bhuyan	Engineering, Integrity & Technical Compliance		Covers IMPS (pipelines?), FIMPS (facilities) & DIMPS
Restoration Verification Audit program	K: drive	FSJ File Room		Akbar Ali Khan	Operational Policy & Environment		Audits of well site reclamation.
Facilities		FSJ File Room	KERMIT	?	Kelowna		
Incidents	K: drive	FSJ File Room	KERMIT	Peter Dalton	Security and Emergency Management		Incidents are tracked in KERMIT, major incidents
ERP (Emergency Response Plans) program	K: drive			Peter Dalton	Security and Emergency Management		
Emergency Response Plans			ERP Database	Peter Dalton	Security and Emergency Management		
Emergency Response Exercises	K: drive			Peter Dalton	Security and Emergency Management		
Security deposits - Liability	K: drive			Wade Abbott / Mike Janzen	Liability Management		
Roads - applications		Application file in FSJ File Room (pre-2016)	AMS (since 2016)	Jody Sutherland	Permitting		
Roads - activity files		FSJ File Room		Jody Sutherland	Permitting		
Pipeline projects - applications		Application file in FSJ File Room (pre-2016)	AMS (since 2016)				
Pipeline projects - activity files		FSJ File Room					
Policies - corporate	K: drive			Julie Barker	Corporate Properties & Administration		
Procedures - according to program							

Geological studies	K: drive	Offsite		Jeff Johnson	Petroleum Geology		
Field and Pool / Reservoir Management	K: drive	Offsite		Ron Stefik	Reservoir Engineering		Covers water disposal, good engineering practice (GEP), concurrent production, waterflood, gas reinjection, experimental/innovative
Production allowable reports	K: drive	Offsite		Ron Stefik	Reservoir Engineering		
External Communication products	K: drive			Graham Currie	Public & Corporate Relations		Covers information letters, industry bulletins,
Annual Reports	K: drive			Graham Currie?	Public & Corporate		
Landowner Liaison	K: drive	Dawson Creek office		Laura-Lea Gibson / Laurie Phillips	Community Relations (Applications)		
Strategic engagement	K: drive			Kelly Wintemute (Indigenous), Corey Jonsson (stakeholder)	Public & Corporate Relations		
Master licences to cut		FSJ File Room		Jody Sutherland	Permitting		
Well files - technical		Offsite	IRIS / E-library	Rob Story	RIS		
Well files - field files / post		FSJ File Room	IRIS / E-library	Terri Marsh	RIS		
Area Based Analysis			ABA	Krista Zens	GIS, Operational Policy & Environment		
Eeyore mapping data			EEYORE	Jody Sutherland	Permitting		
Geospatial data				Krista Zens	GIS, Operational Policy & Environment		
Process Mapping			Process Central	Rob Mitchell	Process Improvement, Analysis & Planning		
Delegation of Authority	K: drive			Lauren Krakau (legal)	Legal Services		
Legal records / cases / etc.	K: drive	Offsite		Sara Gregory	Legal Services		
Major Projects					Major Projects,		

**EXTRA INFORMATION:**

Refer to this document for detailed information: Media notes by ORCS classification:

<file:///K:\RIM%20Victoria\ORCS%20Development%20432-40\OGCO%20ORCS%20Amendment%201\Project%20admin%20and%20background\Media%20notes%20by%20classification.docx>



**EDRMS Needs Assessment**

**For the BC Oil & Gas Commission**

**Version 2**

**April 30, 2021**

**STATEMENT OF CONFIDENTIALITY**

This document is the property of NTT DATA and is produced in response to your request. No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, to parties outside your organization without prior written permission from NTT DATA. For more details, see Legal Notice © 2021 NTT DATA, Inc.

### REVISION HISTORY

---

Version	Effective Date (DD/MM/YYYY)	Brief Description of Change	Affected Section(s)	Prepared By	Reviewed By	Approved By

## TABLE OF CONTENTS

---

<b>1</b>	<b>Executive Summary</b> .....	<b>4</b>
1.1	Key Findings.....	4
1.2	Key Risks .....	4
<b>2</b>	<b>Overview</b> .....	<b>6</b>
2.1	Background .....	6
<b>3</b>	<b>Methodology</b> .....	<b>7</b>
3.1	Compliance Rating System.....	8
3.2	Project Tasks.....	9
<b>4</b>	<b>Findings and Recommendations</b> .....	<b>11</b>
4.1	Records Management Governance .....	11
4.2	Records Classification and Retention Schedule .....	16
4.3	Electronic Records Management.....	20
4.4	Information Protection .....	24
4.5	Information Flow and Retrieval .....	27
<b>5</b>	<b>EDRM System Business Requirements</b> .....	<b>30</b>
<b>6</b>	<b>EDRM Road Map</b> .....	<b>31</b>
<b>7</b>	<b>Conclusion</b> .....	<b>32</b>
<b>8</b>	<b>Acknowledgements</b> .....	<b>33</b>

Appendix A – Questionnaire Results – Summarized

Appendix B – EDRM System Business Requirements

# 1 Executive Summary

In February 2021, the BC Oil and Gas Commission (the Commission) engaged NTT DATA to perform an assessment of business requirements for an Electronic Document and Records Management (EDRM) system to support the management of the Commission's unstructured electronic records, and further the development and enhancement of an EDRM Program and related services.

To prepare this report, NTT DATA conducted a series of data gathering activities. A survey was submitted and workshops conducted with representatives from Records and Information Services (RIS) and Information Technology (IT). The following report is a summary of findings and recommendations as well as EDRM business requirements that comprise the main deliverables of the project.

Based on the Five foundational components of records management, the questionnaire results indicated the following overall maturity level of the Commission's Records Management program:

RM COMPONENTS	MATURITY LEVEL
<ul style="list-style-type: none"> <li>• RM Governance</li> <li>• Records Classification &amp; Retention</li> <li>• Electronic Records Management</li> <li>• Information Protection</li> <li>• Information Flow &amp; Retrieval</li> </ul>	<ul style="list-style-type: none"> <li>• Level 3 (essential)</li> <li>• Level 3 (essential)</li> <li>• Level 1 (sub-standard)</li> <li>• Level 5 (transformational)</li> <li>• Level 2 (essential)</li> </ul>

## 1.1 Key Findings

Much work has already been planned, initiated and, in many cases, completed by the RIS Branch to advance and implement records management best practices and critical foundational work necessary for supporting an EDRM system. For example, the branch has: hired specialist FTEs, modernized the Operational Records Classification System (ORCS) Records Schedule to achieve media neutrality, reflect current standards and the Commission's business environment; engaged an external Records and Information Management (RIM) consultant to classify and schedule unstructured official records stored on shared drives; and developed a wide range of corporate policies, guidelines and educational resources.

It has been evident for some time that the Commission requires appropriate electronic document management tools and additional resources to support the organization in the midst of a rapidly evolving digital business environment. Participants stressed that the current electronic information environment demands controls consistent with EDRM system functionality in order to meet strategic and operational business goals, legislative and policy compliance requirements, and address growing risks associated with information inaccessibility, loss and preservation. The need for an EDRM system has been identified in RIS branch strategic planning documentation (e.g. Information Governance RIM Strategy and Tactical Plan) and included as a project in the Commission's current Corporate Initiatives Register.

## 1.2 Key Risks

A fully implemented EDRM system can protect an organization from significant risks such as data loss, compliance issues, public relations crises, confidentiality breaches, security threats and disaster recovery. A well-executed system helps to mitigate these risks in much the same way that an insurance policy does – by acting as a safeguard against unexpected future events. A comprehensive EDRM system outlined in the recommendations can help to reduce the Commission's exposure to risk in the following areas:

- Decision Making Risk - Not having information available when and where necessary can lead to incorrect decision-making based on incomplete, out-of-date or inaccurate information. Making the wrong decision due to inadequate supporting documentation leads to and may compound the risk exposure in other areas such as financial risk, safety risk and increased costs.
- Financial Risk - Fines can be incurred, money misspent, lawsuits lost, audits unfavorable or opportunities missed when information collections are out of date or incomplete.
- Litigation & Audit Risk – There are a multitude of scenarios involving information management and litigation or audits. Having the appropriate documentation to prove or disprove a claim is one of the key elements to a favorable outcome of an audit or legal action.
- Legislative Compliance Risk – The inability to locate and produce requested records under the Freedom of Information and Protection of Privacy Act (FOIPPA) can lead to formalized complaints, subsequent investigations and potential penalization by the Office of the Information and Privacy Commission. Similarly, non-compliance with the Information Management Act (IMA) can lead to government oversight and intervention. Media reports about legislative non-compliance can contribute towards reputational risk and loss of public trust which would be especially harmful to a regulatory public body.
- Efficiency and Operating Cost Risk – Organizational efficiency can be seriously impaired if needed information is not readily available. Costs for additional staff, office space and records storage can skyrocket when records and document controls are not followed. Also, in the event of litigation or complex audits, internal costs to manage the abundance of ‘documentary evidence’ can be minimized with a well-organized records program.
- Emergency Preparedness Risk - Allowing documents to go unfiled and unmanaged for extended periods of time creates a risk of losing track of vital records in the event of a disaster.

Designed to minimize risk and maximize efficiency and compliance, this report contains detailed recommendations and requirements to improve and manage the unstructured electronic records environment with emphasis on the configuration of an EDRM system for the Commission. These recommendations are practical and reasonable requirements that must be supported by an implementation plan that addresses change management and user support at all stages.

## 2 Overview

### 2.1 Background

The Oil and Gas Commission (Commission) is the provincial single-window regulatory agency responsible for regulating oil, gas and renewable geothermal activities in British Columbia, including exploration, development, pipeline transportation and reclamation. Core responsibilities include reviewing and assessing applications for proposed industry activities, consulting with First Nations, co-operating with partner agencies, and ensuring industry complies with provincial legislation and all regulatory requirements.

The Commission has been rapidly transitioning to become a fully digital organization; however, digital records management has not kept pace. As a result, the Commission finds itself without a system to effectively manage the end-to-end life cycle of its unstructured electronic records (records outside of established information systems).

In addition, the province's legislative framework (Information Management Act) has evolved to modernize and streamline government information management by transitioning to digital storage and information management practices.

#### **Microsoft 365**

The Commission is currently migrating to Microsoft Office 365 (M365) and Azure for enterprise usage. M365 combines a suite of online services, including email, cloud file storage, and secure communication tools along with the traditional desktop applications. A subsequent gap analysis project was anticipated in order to evaluate the commission's records management and user requirements against the functionality M365 offers.

Senior Management understands that well managed information is a valuable and irreplaceable information asset and that in the midst of a rapidly evolving digital business environment, it is essential that records be managed effectively and proactively. For that reason, in February 2021, the Commission engaged NTT DATA to develop "A records management requirements document establishing specific criteria for the Commission, which will serve as the framework for a gap analysis against functionality implemented with Microsoft 365".

The deliverables of this project are the following report of findings, recommendations and EDRM business requirements. Through a balanced combination of objective, quantifiable data and more descriptive, qualitative observations, the report provides the Commission with the essential information it needs to identify gaps and provides a clear benchmark of the functionality required for managing their digital information assets.



### 3 Methodology

This project followed a carefully designed methodology for assessing, developing, and implementing any records management (RM) program. In this case, the methodology has been applied to an EDRM Program. The methodology has been built according to **five foundational components of records management**. The Foundational Components of Records Management comprise a common-sense approach based on the key principles expressed in the International Standard ISO 15489: Information and documentation: Records management.

ISO 15489 is a two-part policy and procedural framework that businesses need to follow to ensure that they create, retain and manage records adequately. Compliance with this standard also facilitates compliance with other ISO standards, such as the broadly recognized ISO 9000 and ISO 14000.

ISO standards reflect the combined work of more than 100 national standards bodies from around the world, facilitating a more efficient exchange of goods and services across borders and legal systems.

By reflecting these universally recognized standards, NTT DATA's methodology ensures not just direct compliance with the ISO standards themselves, but also that electronic records are retained, protected and made available in a way that supports compliance with any applicable laws, regulations and generally accepted practices.

The Five Foundational Components of RM are as follows:



The bulk of this report is organized according to the Five Foundational Components. Each section of the report will explain the Component in more detail, as well as its practical implications for the Commission. Following the details of the Five Components is the EDRM Business Requirements.

### 3.1 Compliance Rating System

For each interview, the Project Team used a rating system to assign a Compliance Score within the Five Foundational Components. These Component scores were then used to complete an overall score for the Commission. NTT DATA developed this rating system to allow for a more objective and consistent assessment of compliance levels. While it is not intended to reflect badly on any particular area, it does allow an organization to see where it is doing well and highlights those areas which will need further enhancements in order to reach a higher level of records management compliance.

The Project Team asked specific questions within each Component to measure how close the Commission is to achieving ideal compliance with the ISO standard. Each answer was given two separate scores. First, an answer was given an objective score based on simple 'yes/no' criteria. Then, the answer was scored more subjectively based on the perceived effectiveness of any practices or documentation linked to that yes/no answer. A summary of questions and responses can be found in Appendix A – Questionnaire Results Summarized.

#### Scoring Table

Score (Yes/No)	Subjective Score	Subjective rationale
Yes (2)	Compliant (2)	Documented processes to meet all key legal requirements and industry standards; Clear, reasonably easy to implement; and Applied to all applicable records
Yes/No (1)	Sometimes/ Informal/Partial compliance (1)	Documented processes but some gaps re: compliance; or No documented processes, but informal practices widely observed.
No (0)	Not Compliant (0)	No documented processes or informal practices; Documented processes but serious inadequacies threaten legislative compliance and/or practical implementation; or Documented processes generally not applied or implemented
n/a (--)	n/a (--)	Given requirement not applicable.

For example, NTT DATA asked representatives whether records are retained long enough to meet legal requirements. The respondents indicated that the Records Schedules are up to date. Although these Schedules are in place, it has not been applied to electronic content. This answer was given a top mark of 2 in the yes/no column, because there are existing Records Schedules, but only a 1 in the subjective column because retentions have not been applied to electronic records. All answers were totaled, and an overall score given for each of the five foundational components.

Are you reasonably confident that records are retained long enough to meet legal requirements and offer defence against litigation risks?	Yes	2	Risk that records have been kept longer due to retentions not being applied to electronic records.	1
Qualitative Score			Subjective Score	

## Maturity Model

While the foundational components identify the critical hallmarks of information management, the Maturity Model defines characteristics of various levels of recordkeeping programs. The five levels of the Model are as follows:

### Records Management Program Maturity Model

#### **Level 1 (sub-standard) 1 – 20 %**

- Record keeping concerns not addressed at all or in a very ad hoc manner
- Organization should be concerned that programs will not meet legal or regulatory scrutiny

#### **Level 2 (in development) 21 - 40 %**

- Developing recognition that recordkeeping has an impact on the organization
- Organization may benefit from a more defined information governance program
- Organization still vulnerable since practices ill-defined and still largely ad-hoc

#### **Level 3 (essential) 41 – 60 %**

- Minimum requirements addressed
- Defined policies and procedures
- Specific decisions taken to improve recordkeeping
- May still be missing significant opportunities for streamlining business and controlling costs

#### **Level 4 (proactive) 61 – 80%**

- Initiating information governance improvements
- Information governance routinely integrated into business decisions
- Easily meets legal and regulatory requirements
- Consider business benefits of global information availability

#### **Level 5 (transformational) 81 – 100 %**

- Routine integration of information governance into infrastructure and business processes
- Recognized effective information governance critical in cost containment, competitive advantage and client service

Although an overall rating can be assigned, most organizations will be at differing levels of maturity depending on the characteristic being evaluated.

## 3.2 Project Tasks

### Start-up Meeting

A start up meeting was held on February 18, 2021. Participants included Kathryn Smerechinskiy, Rob Smith, Mahia Frost and Dana Keough for the Commission and Joan Sparkes and Claire Connelly for NTT DATA. The meeting provided NTT DATA and the Commission an opportunity to discuss project details and ensure consensus with respect to the planned scope, methodology and tasks.

### **Gap Analysis: Structured Data Gathering and Workshops**

The main goal of the project was to understand the current electronic and physical records environment and identify existing gaps and areas of records and information management which would be translated into EDRM requirements. The basis of this assessment was a questionnaire completed by the IS and RIS groups and workshops with the same individuals.

### **EDRMS Business Requirements**

The EDRMS Business Requirements were developed using the Ministry of Management Services Request for Proposal - Enterprise Document and Records Management System as the key point of reference. Although issued in 2001, many of the requirements identified in the Request for Proposal are still functionally relevant today. The Business Requirements were reviewed within a workshop setting and summarized within this report.

## 4 Findings and Recommendations

### 4.1 Records Management Governance

An appropriate corporate governance structure is essential to any records management program which complies with applicable laws, regulations and industry standards. ISO 15489 outlines the key components of a records management governance structure:

- A corporate policy endorsed at the highest level of the executive and defining the authorities, responsibilities, roles and interrelationships of all personnel who manage or perform records management processes;
- A corporate policy statement that provides auditing of compliance with the organization's records management program;
- Designation of one or more individuals at the management-level who will promote, monitor and enforce compliance with the records management program on behalf of the entire organization;
- Clear and direct statement of practices which should be avoided or performed only with special permission from a designated authority;
- Outlining of records management responsibilities in all applicable job descriptions or equivalent documents; and
- An appropriate form and level of training for all designated records management personnel and any personnel with significant responsibility for records creation and/or control.

#### 4.1.1 Findings – Records Management Governance

Overall compliance levels within this Component were as follows:

<b>RM Governance</b>	<b>59% - Level 3 (essential)</b>
----------------------	----------------------------------

Legislative authority for overall records management compliance in the province is provided through the Information Management Act (IMA), an element of which requires the management of government records through information schedules, such as the Administrative Records Classification System (ARCS), Operational Records Classification System (ORCS) and other applicable schedules (e.g., Executive Schedule, Transitory Records Schedule).

As a key governance initiative, ORCS was re-developed as required under the IMA legislation and deemed essential for the appropriate management of Commission records. Approved for use in 2019, ORCS forms the operational framework and modernizes the original ORCS to current standards and

positions the Commission to become EDRM ready. Phase 1 of ORCS development was designed to apply classifications and retentions to most Commission program records saved on the network. Those records remaining will be addressed in ORCS Phase 2.

ORCS Phase 2 development is required under the IMA legislation and for the appropriate management of Commission data and records within systems. Phase 2 entails a detailed analysis of all Commission systems holding operational data and records. As well, the RIS Branch will examine the suitability of ARCS Schedules for administrative, financial, and human resources related information. ORCS Phase 2 has been initiated and is a long-term initiative.

Responsibilities for records management officially come under the jurisdiction of the Director Records and Information Services (RIS) Branch and six full time staff members. There are no dedicated administrative positions outside of this branch. There are individuals that manage their records as part of their overall duties although there is no formal delegation of responsibilities for records outside of RIS.

There are a range of guidelines and policies available on the Commission intranet and a Confidential Information Management Guide forms part of the annual sign-off process with the Code of Conduct for each employee. Additional materials are currently under development (e.g. Digitization Policy, Email Management Guide).

The entire Commission organization was trained in elements of the IMA through Documenting Commission Decisions workshops. The ORCS development process familiarized some areas with information schedules. Program specific RM training has been provided on an as-needed basis as well as training and information sessions on Freedom of Information and Protection of Privacy Act (FOIPPA) requirements.

## 4.1.2 Recommendations – Records Management Governance

NTT DATA recommendations for the Commission under the Component of Records Management Governance are divided into four areas:

### 4.1.2.1 EDRM Roles and Responsibilities

To support an EDRM Program, consider establishing a dedicated EDRM Business Analyst, on either a full time or contract basis. In collaboration with IS, the role of the business analyst is to support the planning, introduction and roll out of the new EDRM system. Within context of EDRM functionality, the Business Analyst would be responsible for the following:

- Examine existing business processes and identify critical records collections,
- Identify gaps in processes and opportunities for improvements and automation,
- Capture requirements, create site mockups,
- Generate technical requirements, proof of concept solutions,
- Help implement the new processes, features, and tools, and

- Document improvements, measure progress, repeat the process, and
- Deliver training to users on system functionality.

Directly address day-to-day Department Site Administration records management responsibilities (e.g. maintaining electronic file directories, granting permissions to Team Sites) as part of the position responsibilities for administrative support personnel, where appropriate.

#### 4.1.2.2 EDRM Procedures and Best Practices

The Commission will be required to develop EDRM procedures to direct the program. The focus will be on the development of detailed department specific work procedures and practices on such topics as:

- Document repository overview – ‘where to store’ rules i.e. EDRM/OneDrive/etc
- Navigating the EDRM System and Department Sites
- EDRM Roles and Expectations
- Classifying and Naming Department Specific Electronic File Collections
- Adding and revising documents within EDRM
- Sharing documents from EDRM
- Searching the EDRM repository

#### 4.1.2.3 EDRM Training and Awareness

Concurrent with the completion of EDRM procedure and practices, it is recommended that the Commission develop a EDRM Training and Awareness Plan to proactively ensure compliance with its program. Appropriate training and awareness materials should be provided to all staff with responsibility for records and should be customized for the type of User. The following is an example of the different types of training which may be offered:

Staff Category	Time	Example of Topics Covered
New Employee Orientation	15 – 20 mins – part of on-boarding	<ul style="list-style-type: none"> <li>- Provide RIS Welcome Package</li> <li>- Identify contacts – who to contact for help or more information</li> <li>- Schedule follow up in 3 weeks after hire date to conduct more in-depth training at that time.</li> </ul>
EDRM Basics	30 minutes	<ul style="list-style-type: none"> <li>- RM benefits &amp; need for compliance</li> <li>- EDRM responsibilities</li> <li>- ARCS/ORCS Overview</li> </ul>

Staff Category	Time	Example of Topics Covered
EDRM Advanced – Department Specific Content	1 hour	<ul style="list-style-type: none"> <li>- EDRM System Overview/Where to Store?</li> <li>- Navigating, Searching, Adding, Revising Content</li> <li>- RM benefits &amp; need for compliance</li> <li>- EDRM responsibilities</li> <li>- ARCS/ORCS Overview</li> <li>- EDRM System Overview/Where to Store?</li> <li>- Navigating, Searching, Adding, Revising Content</li> <li>- Collection specific naming conventions, metadata, workflows as needed</li> </ul>
EDRM Administrative Support - Department Specific Content	1.5 hours	<ul style="list-style-type: none"> <li>- RM benefits &amp; need for compliance</li> <li>- EDRM responsibilities</li> <li>- ARCS/ORCS Overview</li> <li>- EDRM System Overview/Where to Store?</li> <li>- Navigating, Searching, Adding, Revising Content</li> <li>- Collection specific naming conventions, metadata, workflows as needed</li> <li>- Granting permissions, understanding security classifications</li> </ul>

**4.1.2.4 EDRM Program Assessment Process**

Following the implementation of the recommendations for user training and support, it is recommended that the Commission develops and deploys an EDRM Program assessment process. The EDRM Program Assessment will act to monitor success of, and adherence to the EDRM component of the Records Management Program and to identify and minimize the organization’s exposure to risks inherent in the future management of large decentralized collections of electronic records using the new EDRM tool. The assessment will provide a baseline on user adoption and compliance and is a proactive approach to continuous process improvements.

The purpose of an assessment process is:

- Provide information about the efficiency and effectiveness of the EDRM Program as a whole and of the individual procedures that make up the program;
- Measure accuracy and adherence to program standards;
- Highlight problem areas; and
- Provide a basis for corrective action of both department practices and the EDRM Program itself.

NTT DATA recommends that the Commission’s EDRM Program assessment consist of the following three components:

- Periodic Department Assessments
- Annual Department Assessments



- Program Assessments

Periodic department assessments can be conducted bi-annually or more frequently if necessary and Department and Program assessments conducted annually. User surveys, checklists and examinations of files and electronic environments (as some examples) are methods that can be used to complete the assessment. At all times, the Assessments must be objective, measurable, and used as opportunities to support and assist the Departments to better manage their information. The Assessment Program and details of the scope and measures should be shared with Department Managers and Administrative Support Staff once they are finalized and prior to conducting an Assessment.

### **4.1.3 Summary – Records Management Governance**

The following summarizes the recommendations within the Records Management Governance Component as it relates to EDRM at the Commission:

- Establishment of a dedicated EDRM resource person
- Explicit Identification of EDRM Responsibilities for all staff as applicable
- Review and development of EDRM Procedures and Best Practices
- Development of EDRM Training and Awareness Program
- Development of EDRM Program Assessment Process

## 4.2 Records Classification and Retention Schedule

The Commission's records management program is built largely around the ORCS and ARCS, which categorizes records by subject or activity and defines how long records are to be stored before they are destroyed in compliance with applicable laws, regulations and other business requirements. The Commission adopted ORCS and ARCS upon its inception in 1998 through inherited collections of records from existing Ministries and continues to update its ORCS to address unscheduled and/or new business areas and activities.

ISO 15489 explains some of the main features of a compliant Records Classification and Retention Schedule:

- Organizing records according to the business activities of which they provide legal evidence
- Providing a conceptual basis for the reliable retrieval of records
- Assigning responsibility for particular sets of records to appropriate groups within the organization
- Establishing records retention periods and appropriate methods of final disposal and/or storage

In assessing the Commission's compliance with this Component, with focus on its unstructured electronic records, the Project Team explored three main issues:

- Degree to which each Department had successfully applied the Records Classification and Retention Schedule to its business records;
- Whether various content elements within the classification (categories, headings, scope notes, responsible departments) still accurately provided for the business functions, activities, and records of the office; and
- Whether records retention periods still provided for the operational needs or known legal/regulatory requirements for keeping records.

### 4.2.1 Findings – Records Classification & Retention Scheduling

Success levels in applying and implementing the Records Classification and Retention Schedules varied across different offices and Branches. Some areas have applied ARCS/ORCS to both hard copy and electronic documents while others have not implemented the system at all.

The overall compliance levels under the Component of Records Classification and Retention Scheduling as it relates to unstructured electronic records were as follows:

<p><b>Records Classification &amp; Retention Scheduling</b></p>	<p><b>52% - Level 3 (Essential)</b></p>
---	---

#### 4.2.1.1 ORCS Update Phase 1 - Completed

As a Phase 1 initiative, ORCS was re-developed as required under the IMA legislation and deemed essential for the appropriate management of Commission records. Approved for use in 2019, ORCS forms the operational framework and modernizes the original ORCS to current standards and positions the Commission to become EDRM ready. Phase 1 was designed to apply classifications and retentions to most Commission operational program records saved on the network. Those records remaining will be addressed in ORCS Phase 2.

#### 4.2.1.2 ORCS Update Phase 2

ORCS Phase 2 commenced in fiscal 2020/21 and involves a detailed analysis of all Commission systems holding operational data and records. The Commission has a complex and ever-changing system environment. New systems are being initiated on a continual basis. A review of each operation system is necessary for ensuring IM compliance and retention planning has been addressed. As a Phase 2 initiative, existing approved records schedules (ARCS, Human Resource ARCS Supplement - HRAS) will be assessed for suitability for the Commission's administrative records with the potential of creating new customized schedules to address record retention needs.

ORCS Phase 2 development is required under the IMA legislation and necessary for the appropriate management of Commission data and records. Phase 2 is ongoing and recognized as a long-term initiative.

#### 4.2.1.3 Unstructured Electronic Records

The Commission's shared drives (e.g. K: Drive) and Outlook (email) are being used as an unstructured recordkeeping system throughout all offices and Branches. The challenge is steadily increasing as more records are created and received. Information related to and supporting business functions is fragmented and staff experience difficulty locating records needed for their work or may not have access to the information they need for decision-making purposes. A summary of risks operating in this type of information environment may be summarized as follows:

- Inability to locate critical information;
- Non-compliance with applicable IMA and FOIPPA legislation, policy and best practices;
- Destroying records before they are legally eligible for destruction (not keeping records long enough);
- Keeping records longer than required thus creating risks associated with FOIPPA and document production under litigation (e.g. having to produce records that legally could/should have been destroyed);
- Mixing transitory information with official records; and
- Lack of protection for personal and/or sensitive confidential information.

Management recognized the need for appropriate classification and reorganization of electronic records to address these issues as well as for future EDRM implementation. Commenced in 2018/2019, a contract was initiated with a RIM consulting company to organize shared drive records according to ARCS/ORCS on a program-by-program basis. This critical work was paused for 2020/21 due to the uncertainties associated with Covid 19 and is resuming for fiscal 2021/22.

#### 4.2.1.4 Records Searches

Another major finding is that the Commission does not currently use an automated records management system. There is currently no ability to search or index records across the organization. The Commission

must routinely respond to time-sensitive FOIPPA requests, and requests for records by counsel and in response to litigation. Not having these records indexed makes it difficult to respond in a timely manner. The RIS Branch FOIPPA Specialist(s) works collaboratively with all levels of staff on FOIPPA requests, and with Legal Services to support their requirements.

Conducting adequate and thorough searches for records across the Commission can be challenging due to the fragmented, siloed and unstructured state of its records. A typical request involves searching multiple repositories, systems and information locations and there is a real risk that not all information is being located/produced.

In an organization the size of the Commission, the task of effectively and efficiently managing and controlling records without automated tools such as an EDRMS is extremely difficult if not impossible, and creates the following situations:

- Difficult and time consuming to determine the ownership, location or existence of records;
- Decreased decision-making ability due to inefficient access to information resources;
- Increased storage and retrieval costs because content is not tracked and indexed;
- Unnecessary labour costs to perform easily automated manual tasks such as transferring files offsite and creating file listings; and
- Overwhelming difficulties enforcing legislative responsibilities and consistent record keeping practices.

Having records identified incorrectly or not identified at all increases the risk of not being able to find information, loss of credibility as a public institution and obvious time wasted searching for records.

## **4.2.2 Recommendations - Records Classification & Retention Scheduling**

### **4.2.2.1 Shared Drive Implementation Plan**

Already a key part of the existing RIS branch EDRM readiness plan, it is recommended that the Commission continue with the ongoing classification of electronic program records. This work is of high value to the Commission. Most of the program records are considered critical collections and an organized shared drive is not only foundational preparation for a future EDRM project, but key to securing and protecting the Commission's information assets over the long term.

It is further recommended that the Commission take a more direct and focused approach within all areas to organize shared drives as a whole. Currently, the Commission approaches shared drive projects with a two-pronged approach: "do-it-yourself" (DIY) projects completed by program staff with guidance from RIS branch; and a series of formal guided projects lead by the contracted RIM consultant. |

When the Commission initiated its shared drive organization project in 2017/18, it was decided that Human Resources would serve as the pilot area. Since then, a systematic approach to folder cleanup, organization, and classification structure has been applied to each subsequent program area. Selection of areas has been ad hoc, based on operational cycles and client readiness. To date, the Commission has completed a total of six projects with the RIM consultant with a seventh project underway.

It is recommended that a comprehensive Shared Drive Implementation Plan be initiated to drive the cleanup of all network directories. An Implementation Plan may serve to formalize the process and communicate the benefits of the work across the organization.

A Shared Drive Implementation Plan involves the purging and restructuring of shared electronic directories within the MS Windows environment. The benefits of cleaning up network drives are as follows:

- Organizes collections of active records that reflect individual department responsibilities and accountabilities;
- Removal of outdated and redundant documents no longer needed;
- Addresses and secures a home for the “orphaned” content;
- Supports compliance and reduces risk;
- Increases efficiency when locating information;
- Facilitates information sharing and collaborations; and
- Readiness of critical document collections for conversion to more advanced document management technologies.

The recommended approach is to start with a Pilot area to demonstrate the concepts and folder design principles for the Pilot Department shared drive. Although similar in design, each Department will require an electronic folder structure customized for their particular content. The Program records cleanup will augment this initiative. The objective is to have consistent, compliant practices within each business area.

As a minimum, the Shared Drive Implementation Plan should include the following elements:

- Enrollment - introduce the Branch in the initiative and agree on a timeline / schedule for completion
- Content Analysis - Existing shared drive folders, directory tree structures, program structures (existing)
- Design - Drafting suggested new folder structures/sub structures
- New Environment Set Up - Establish new folder structures for the Branch in their existing directories
- Training – Offer workshops, deskside support and User documentation on naming standards, folder design principles and best practices for using an electronic shared environment
- Support - Regular monitoring of progress of clean up and assistance as needed

#### **4.2.2.2 Records Searches**

As part of this initiative, business requirements have been identified to address functionality for an EDRM system which includes tracking and control of record holdings to support records searches. See Appendix B.

#### **4.2.3 Summary – Records Classification and Retention Scheduling**

The following summarizes the recommendations within the Records Classification and Retention Scheduling component of records and information management at the Commission:

- Shared Drive Implementation Plan
- Implementation of an Electronic Document and Records Management (EDRM) system to support records searches

### 4.3 Electronic Records Management

British Columbia, along with most legal jurisdictions, defines a 'record' as recorded information in any medium or format. As such, legal definitions do not distinguish between paper and electronic records, therefore organizations must apply the same records management standards to their electronic information systems as to their paper files. However electronic recordkeeping does introduce new challenges which warrant special attention in this report. In assessing how well the Commission responded to these challenges, NTT DATA explored the following questions:

- Are computer drives, folders and other such structures organized according to a standardized taxonomy which assists in compliance with ARCS/ORCS and allows staff to find records and information to support their activities?
- Are emails managed and retained according to Commission records management policies?
- Are strategies in place to minimize the duplication of information, in terms of both multiple electronic records and between paper and electronic versions?
- Does the Commission have a version control procedure or tools to help identify when a document becomes an official record?
- Are digital images of paper records created according to a controlled process which ensures the reliability of the image as a substitute for the original?

#### 4.3.1 Findings – Electronic Records Management

To date, the Commission has made limited progress in systematically applying ARCS/ORCS to the Program records, documents and data created and stored on electronic systems. Outside of the Commission's operational information systems, there is heavy reliance on shared drives as recordkeeping repositories. Additional concerns with respect to electronic document management dealt with the management of data contained on email and personal computing devices.

Coming in with the lowest overall rating for the Commission, compliance levels under this Component are as follows:

**Electronic Records Management**

**13% - Level 1 (sub-standard)**

##### 4.3.1.1 Reliance on Shared Drives

Electronic business documents are stored primarily on shared drives. As noted, the RIS Branch has engaged a RIM consultant and supported several Program areas in developing and implementing electronic folder structures that mirror the ARCS/ORCS classification structure. Once complete, adherence and ongoing maintenance of these folder structures is left to individual and/or department practices. Overall IT network administrators provides access and security to these electronic folder collections. The Windows environment does not have version control or document sharing capabilities.

The electronic records at the Commission are not subject to automated removal for inactive storage or deletion. While network backups are handled on a regular basis, the contents of the network drives or data contained within software applications are not being managed from a records management standpoint.

With no centralized control or tools for applying standards, users across the organization have encountered challenges with redundant copies, competing versions, and difficulty locating information due to inconsistent naming conventions and personalized folder structures.

Long term management and ongoing preservation of scanned records is also an issue. The Commission routinely converts high volumes of hardcopy records held in historical asset and application files (e.g. well, pipeline, facility and associated application files, as well as other ancillary applications) to digital format for internal and external client use. For some records, their provision is a legal obligation under the Oil and Gas Activities (OGAA) General Regulation and forms part of the Commission's mandate. Digital copies of scanned historical asset records are included amongst the electronic records saved on shared drives.

#### **4.3.1.2 Email Management**

The Commission, like many organizations, experiences inconsistent business e-mail management practices across the organization. The Commission currently limits the size/amount of employee e-mails. Some business areas delete emails to comply with the size limitations while others are letting messages aggregate uncontrollably inside their MS Outlook e-mail environments.

### **4.3.2 Recommendations – Electronic Records Management**

#### **4.3.2.1 Continue Organizing Shared Drives**

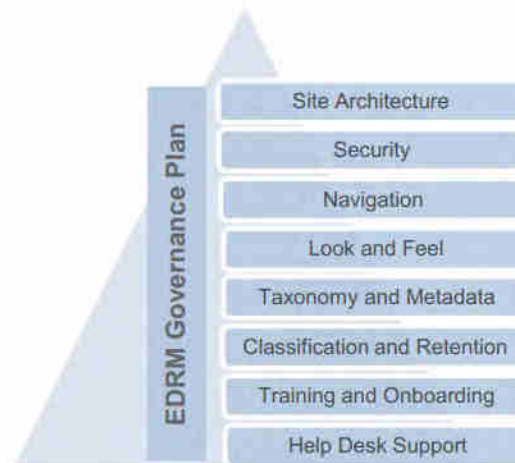
NTT DATA recommends that the Commission continue its work in implementing the shared drive reorganization process as described in the previous section 4.2.2.1. Standard folder structures and naming conventions for the storage of electronic information should be designed in parallel with the ARCS/ORCS structure and applied for all records in every program and business areas. The stretch goal is to have all Commission electronic documents, program and administrative related, fully classified and naming conventions applied prior to migration to EDRM.

#### **4.3.2.2 Develop An Electronic Content Management Strategy**

Once the shared drive reorganization process has progressed, the Commission will be well positioned for implementation of an Electronic Document Records Management (EDRM) system. EDRM encompasses the management of electronic records, documents and e-mail, including version control, security and authenticity assurance. These tools are not a solution in themselves – and RIS, IT and Users need to remember that the proper application of records management principles along with building well-designed structural elements will ensure the success of any system adopted.

One of the basic components of any EDRM strategy is the Records Classification and Retention Schedule scheme. Once information is migrated to an EDRM platform, electronic document collections can be 'tagged' and meta data applied such as retention code, department name, etc. that will allow for more robust information reporting, management and searching. However, whether information is stored electronically or in paper, tracked manually or with advanced document management technologies, the same principles of organization, consistency and control must be applied.

While the technical functionality of these systems is important, the application, design and deployment of the software are vital to its acceptance, use and control by the business areas. NTT DATA recommends the development of an EDRM Governance Plan to establish minimum rules of engagement, procedures and guidelines related to the use and administration of the EDRM system which would address the following general areas:



It is further recommended that any system be piloted on a small collection to evaluate the usability of the system and to identify any issues to be addressed prior to full implementation.

As part of this initiative, business requirements have been identified to address functionality for an EDRM system. See Appendix B.

#### 4.3.2.3 Apply E-Mail Best Practices

Enterprise email management systems are part of an overall solution and are interdependent with the Commission's EDRM strategy which will address automated email archiving. Until these tools are available, it puts undue pressure on individual employees to manually process and organize the increasing volume of email back log.

Following the implementation of EDRM and the associated email management solution, email messages can be migrated to appropriate electronic records storage locations within the EDRM system. As a result, the messages would become available for access / sharing across a team or business area yet still would be managed by automated records governance rules of classification and retention.

The RIS branch is developing an email management guide to support staff in email management best practices. Currently, recommended records management practices involve deleting transitory emails and filing official email records to applicable shared drive recordkeeping systems.



As an interim step, NTT DATA recommends that RIS raise the awareness of email best practices such as definition of business emails, proper use of Subject Lines, handling attachments, saving emails to the network, creation of folder structures within Outlook, sender's responsibilities for saving, management of inbox traffic, deletion of non-business and transitory emails, etc. The principals and practices for properly managing emails will continue to apply with or without an email management solution.

### **4.3.3 Summary – Electronic Document Management**

The following summarizes the recommendations within the Electronic Document Management Component of records and information management at Commission:

- Continue Organizing Shared Drives
- Develop An Electronic Content Management Strategy
- Apply Email Best Practices

## 4.4 Information Protection

The component of Information Protection refers to a wide range of storage devices and facility features that help protect computing devices, paper and other records media from loss, damage and unauthorized access. Such measures support the other four RM Components of Compliance by ensuring that records are kept accessible, confidential and reliable for as long as business dictates. In assessing the Commission's compliance within this Component, NTT DATA addressed questions such as:

- Are you aware of or familiar with any disaster recovery or business continuity plans?
- Are paper files and other media stored in enclosures and/or facilities which prevent access by unauthorized persons?
- Are offices and records storage areas equipped to mitigate the risks of loss or damage due to fire, floods and other emergency situations?
- Are records of long-term value sufficiently protected against environmental degradation and user wear and tear?

### 4.4.1 Findings – Information Protection

Facilities and practices related to Information Protection scored the highest of all components surveyed. Overall compliance with this Component were as follows:

<b>Information Protection</b>	<b>83% - Level 5 (Transformational)</b>
-------------------------------	---

#### 4.4.1.1 Business Continuity Plan and Vital Records

At this time, there is a documented Business Continuity Program (BCP) for the Commission and vital records have been identified within the context of this plan. Communication with Program areas as to the identification and protection measures required for vital records come under the purview of the BCP Director.

As stipulated in the BC Government's Core Policies and Procedures for Information Management and Information Technology Management, the following are requirements relating to vital records and information technology business continuity plans:

- Government must create and maintain a business continuity plan that includes identification and management of its vital records.
- Vital records must be maintained so that re-establishing the legal, financial and functional responsibilities of government is achieved quickly after a catastrophic event or crisis.
- Vital records must be maintained in a manner that meets current environmental and security standards.
- Ministries must develop, or work with their supporting infrastructure technology service providers to develop Business Continuity and Disaster Recovery Plans on all information systems and the associated technology infrastructure and test them regularly.

Repercussions arising from the inability to recreate vital records may include the following:

- Reduction or loss of financial revenue;

- Reduction or loss of organizational productivity, including creation and provision of goods and/or services;
- Disruption in customer service;
- Increased exposure and vulnerability to litigation-related factors, such as lawsuits and legal penalties;
- Reputational damage; and
- Unexpected administrative and other financial expenses.

Vital records within the Commission have been identified, and include well files, pipeline files, application files, facility files, pay and financial records. The centralized records centre in Fort St. John holds the physical copies of these records (well, facility, application and pipeline files) and older financial and legal records are maintained in government contracted storage facilities. These facilities were purpose built for this function, with fire suppression and safety measures in place. Electronic records considered vital are protected by IT through regular network or system back up processes.

#### 4.4.1.2 Information Security Classification

The provincial Information Security Classification Standard provides a common standard for security classification of government information. As shown in the following table, this standard describes four levels of security classification to be applied to government information based on the degree of harm that could reasonably be expected to result from unauthorized disclosure.

Within IT, network security and permissions are handled by controlling access to specific network resources, shared drives, systems or applications for individual users or groups. Information security is handled on a per system basis.

	Level	Description
PUBLIC		No harm to an individual, organization or government Examples: Job postings, communications to claim clerks, business contact information, research and background papers (without copyright restrictions)
CONFIDENTIAL	Protected A	Harm to an individual, organization or government Examples: Home addresses, dates of birth, other low-risk personal information
	Protected B	Serious harm to an individual, organization or government Examples: Law enforcement and medical records, personnel evaluations and investigations, financial records, information subject to solicitor-client privilege or other legal privilege
	Protected C	Extremely grave harm to an individual, organization or government Examples: Information about police agents and other informants, Cabinet records or Cabinet-related records

## **4.4.2 Recommendations – Information Protection**

### **4.4.2.1 Strategy for Vital Electronic Records Protection**

An EDRMS will support the protection of vital electronic records. The Commission has sound protections in place for its physical vital record holdings, however it also needs to protect the authenticity, integrity and stability of the electronic vital records. Appropriately storing electronic vital records ensures they are backed up on a secure storage device and the Commission can be assured that the vital records holdings within their custody are safely protected for generations to come.

### **4.4.2.2 Adoption of Security Classifications**

Within the context of EDRM Governance Plan described in Section 4.3.2.2, the recommended security classifications must be adopted and applied to content migrated to this system. As part of an overall Security governance model, mandatory metadata such as security roles and confidential classifications of data elements will ensure the protection of confidential information across all business areas.

## **4.4.3 Summary – Information Protection**

The following summarizes the recommendations within the Information Protection Component of records and information management at the Commission:

- Strategy for Vital Records Protection
- Adoption of Security Classification

## 4.5 Information Flow and Retrieval

The Component of Information Flow and Retrieval encapsulates a number of practical needs that an organization must address in order to comply with requirements and manage its business more efficiently. Among the key criteria assessed under this Component were:

- Overall assurance of timely access to and retrieval of records needed for daily business decision-making;
- Ensuring that records are accessible only to those who have a genuine need to access that information for purposes of completing authorized activities, as mandated by privacy laws and proprietary business rules;
- Minimizing storage costs and retrieval time by transferring inactive records to a more cost-effective location; and
- Ensuring that all relevant records, both active and inactive, will be located and retrieved in the event of a litigation, audit or personal information access request under applicable laws.

### 4.5.1 Findings – Information Flow and Retrieval

Rating in the Component of Information Flow and Retrieval varied greatly between Departments. Overall compliance levels under this Component were as follows:

Information Flow and Retrieval	55% - Level 3 (Essential)
--------------------------------	---------------------------

While the Commission lacks some of the formal tools for managing records throughout the different stages of their lifecycle, some areas have achieved an adequate degree of control over active and inactive records. Within the Component of Information Flow and Retrieval, NTT DATA noted the following key areas for improvement:

#### 4.5.1.1 Information Silos and Fragmentation

Clear interdependencies are well supported, but siloed information exists as a product of the separate and distinct systems and personal work habits (e.g. outlook, personal drives, unmanaged shared drives). Disjointed records collections make it difficult to manage the information within context of the whole and makes retrieval and identification of file contents inaccurate and inconsistent. This condition exists in both hard copy and electronic environments.

Major records streams are fairly consistent and therefore easier to access (supported by centralized file rooms for physical records and systems for digital information). Outside of the main program areas or when searching for information outside of the User's home Department, siloed information practices present challenges in locating records.

#### 4.5.1.2 Records Searching

It is difficult for the RIS staff to do basic record searches and retrievals with confidence. RIS Branch staff face a complicated, multi-step process for searching, locating and retrieving active and offsite records. Multiple versions of excel tracking spreadsheets are maintained by the records management staff for locating offsite records and there is heavy reliance on records staff to interpret data contained within the

multiple spreadsheets and locate records. There is a risk when responsive records must be produced within rigid time limits for FOIPPA or litigation, and it is not clear that all information has been located.

#### **4.5.1.3 Unmanaged Working Files**

Users tend to create Working files for cross-functional activities such as projects, proposals, draft legislation, etc. For the most part, these interim files are not entered or tracked anywhere within ARCS/ORCS making it difficult to search for the location of information before close out or completion of the project or activity. While not a concern for many short-term activities, it does create difficulties with files created for long term projects or strategic developments and increases the risk on not being able to find required records in a timely manner. As well, the shared drive has no version control abilities, so it is very difficult to identify and control the latest and most complete versions of documentation.

### **4.5.2 Recommendations – Information Flow and Retrieval**

The Commission should take the following steps to better control the flow of information and support overall business efficiency:

#### **4.5.2.1 Content Mapping for Critical Collections**

To address fragmentation and file integrity issues across the Commission for critical collections, NTT DATA recommends that Commission initiate the identification and documentation of locations of file collections for each Program area. Information to be captured for each collection would include such details as:

- Official Title of Collection
- Owner / Custodian
- Naming Conventions / Indexing
- How Organized / Folder or Document Sub Structures / Taxonomies if any
- Document Types and media (h/c, electronic, system of record)
- Permissions
- Location(s)
- Retention Period

The organization and cleanup of electronic program records currently being conducted will greatly contribute to this initiative.

#### **4.5.2.2 Working File Administration**

For multi-departmental long-term projects and initiatives, encourage Users to manage their Working Files within an ARCS/ORCS structure and create a process to merge and purge Working Files following project completion and close out with the Project Lead. The management of working files will become much easier following the implementation of EDRM.

#### **4.5.2.3 Offsite Records Tracking**

The RIS Branch would benefit from a simple/searchable database that contains all key information related to the Commission's offsite record holdings, which an EDRM will provide. This will address access issues, reduce risk of non-compliance associated with records searches, and ensure accurate information related

to offsite record holdings is available. The requirements for this functionality are addressed in the EDRM business requirements found in Appendix B.

### **4.5.3 Summary – Information Flow and Retrieval**

The following summarizes the recommendations within the Information Flow and Retrieval Component of records and information management at the Commission:

- Content Mapping For Critical Collections
- Working File Administration
- Offsite Records Tracking

## 5 EDRM System Business Requirements

EDRM encompasses the management of electronic records, physical documents and e-mail, including version control, security and authenticity assurance. One of the basic components of any EDRM strategy is the Records Classification and Retention Schedule scheme. Once information is migrated to an EDRM platform, electronic document collections can be 'tagged' and metadata applied such as retention code, department name, location, etc. that will allow for more robust and secure information reporting, management and searching.

Guiding principles for the selection of an EDRM system include:

User Friendly – To support high user adoption, the EDRM system must be logical to operate and simple to learn. The interface must be consistent across all windows, menus, functions and commands. It must be intuitive to navigate and search, with as few mouse clicks and keystrokes as possible. It must also be accessible both on the desktop and in a web browser.

Classification Inheritance – The EDRM system must have the ability to automatically capture and apply records classifications to content in the background, without infringing on usability for end users. In essence, it must allow users to manage and store their information in the EDRM repository in a way that is meaningful and aligned to their business process and practice, while the system captures and classifies it in the background.

Robust Security and Audit Capabilities - The system should allow for varying levels of access, where sensitive, private or classified information can be restricted so that only specific individuals within the Commission can view or use it. The EDRM system should always prevent the unauthorized destruction or deletion of registered physical and digital records and associated metadata. The system must also provide audit trails of who had access and the actions taken on the records.

Manage Electronic, Physical and Hybrid Records – The EDRM system must be able to manage physical files as well as electronic records. These functionalities enable the management of the physical location of records in the form of paper files, tapes, disks, reports and archive boxes, and their storage locations, which may include filing cabinets, offsite commercial storage locations, and archival repositories.

Implementing EDRM within the Commission will not only to make it easier to locate documents and records, but also for future document control and advanced record management practices. EDRM software solutions integrate all current business document management into one seamless, centralized electronic records system.

EDRM System Business Requirements are detailed in Appendix B.

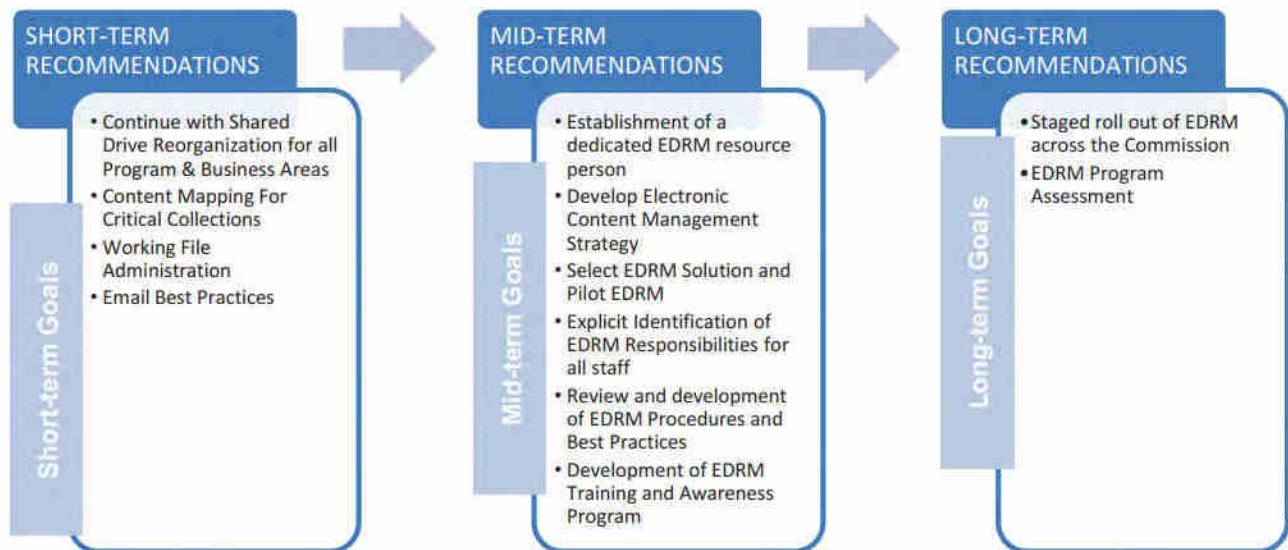


## 6 EDRM Road Map

The recommendations that are presented in this report should be considered as pieces belonging to an overall Commission EDRM deployment strategy. The overall prioritization and execution of changes to how information is being handled must be driven by an integrated, comprehensive and well supported plan much more encompassing than what was included in this study.

NTT DATA acknowledges the Commission already has in place many components of a comprehensive Records Management Program however, it is important for the Commission to consider the actions outlined below in order to obtain a fully compliant EDRM Program as they move into an increasingly complex electronic information management environment.

The following summarizes the suggested priorities and time frames for the implementation of recommendations to mitigate risk in the most optimized manner in terms of short-, mid-, and long-term goals.



## 7 Conclusion

NTT DATA's EDRMS Needs Assessment examined different facets of the Commission's tools and practices for managing its electronic records. The assessment found that while the Commission already has many key foundational practices in place, there are several important actions to take or continue before its records can fully support business efficiency and manage operational risks across the organization.

Implementation of an EDRM system to store and preserve its critical administrative and operational records collections, supported by the continued cleanup and reorganization of shared drives are strategic measures for advancing information management practices at the Commission.

While applying these recommendations is a significant task, doing so will bring tremendous return-on-investment in the form of improved business efficiency, legal and operation risk management, and accountability. NTT DATA is always pleased to provide further information and welcomes further opportunities to partner with the Commission in realizing these benefits.

## 8 Acknowledgements

NTT DATA would like to graciously thank Kathryn Smerechinskiy, Rob Smith, Mahia Frost and Dana Keough for their support and guidance throughout this project. NTT DATA is proud to partner with the Commission to support their records management initiatives and looks forward to continuing the successful relationship as they grow and expand their records management program.

Records & Information Services (RIS) Branch Planning for Fiscal 2024/25  
**Summary of Key FOIPPA and Records Management Issues, Risks & Gaps to Assess Project Priorities & Resource/Funding Requirements**

March 27, 2024

Table of Contents

**EDRMS READINESS**

1. ORCS Development – Phase 2: Creation of System Overviews & Assessment of Program Areas for ARCS Applicability
2. Organization/Clean-Up of Electronic Program Records on Shared Drive(s) in Accordance with ARCS/ORCS

**DATA DEFRAGMENTATION STRATEGY - DIGITIZATION**

3. Addressing the Hardcopy Well Files and Well Data Fragmentation Problem: Creation of Data Source Roadmap to Identify Locations of Relevant Well Data/Records
4. Addressing the Hardcopy Well Files and Well Data Fragmentation Problem: Conversion of Pre-2014 Records from Hardcopy to Electronic Format
5. Addressing the Commission's Hardcopy Well Files and Well Data Fragmentation Problem - Risk of Legislative Non-Compliance: Well Log Records
6. Addressing the Hardcopy Well Files and Well Data Fragmentation Problem - Risk of Legislative Non-Compliance: Pressure Test Records
7. Conversion of Hardcopy Field & Pool Files to Electronic Format - Digitizing Key Record Series Maintained/Utilized by Reservoir Engineering & Geology Staff

**FILE INTEGRITY**

8. External Release/Publication of Well Information: Appropriate Management of the Two Sets of Well Files Maintained by Victoria and FSJ Offices

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
<b>Foundational Elements / EDRMS Readiness</b>									
1		<b>ORCS Development – Phase 2:</b> Creation of System Overviews & Assessment of Program Areas for ARCS Applicability	<ul style="list-style-type: none"> <li>• ORCS Phase 2 will involve:                             <ul style="list-style-type: none"> <li>– Detailed analysis of all Commission systems holding operational data and records. This enables identification of retention plans for structured data held in Commission information systems (as well as GIS data).</li> <li>– Addressing any gaps within the ORCS structure; the ORCS structure may change as a result of understanding how records are currently managed within systems, or how they will be managed in the future.</li> <li>– Assessing the suitability of existing approved records schedules (ARCS, HRAS) for the Commission's "administrative" records; the development of new customized schedules may be required to address record retention needs.</li> </ul> </li> </ul> <p>Phase 1 was completed, and ORCS approved in 2019.</p>	High	<ul style="list-style-type: none"> <li>• The BCER has a complex and ever changing system environment – new systems are being initiated on a continual basis. A review of each operation system is necessary for ensuring IM compliance and retention planning has been addressed. System Overviews are a requirement of the ORCS structure and subject to the provincial approval process.</li> <li>• The ORCS only applies to Commission operational records. Administrative records also need to be appropriately addressed through the use of existing schedules or creation of customized Commission-specific ones.</li> </ul> <p><i>Administrative records relate to: finance, building/property administration, business planning, Board materials, IT/IS activities, internal audit, HR, etc.</i></p>	<ul style="list-style-type: none"> <li>• <b>Commence Phase 2 in Q4 of fiscal 2024/25 (secondment).</b></li> <li>• Phase 2 work is extensive and anticipated to require 1-2 years to complete.</li> </ul>	<ol style="list-style-type: none"> <li>1. ORCS Phase 2 development is required under the IMA legislation and appropriate for the appropriate management of Commission data and records within systems.</li> <li>2. Appropriate classification and retention of Commission administrative records is necessary for EDRMS implementation.</li> </ol>	Pending	Digital Information Management Specialist
2		<b>Organization/Clean-Up of Electronic Program Records on Shared Drive(s) in Accordance with ARCS/ORCS</b>	<ul style="list-style-type: none"> <li>• Commission shared drives (e.g. K: Drive) and Outlook (email) are being used as recordkeeping systems</li> <li>• This is a Commission-wide problem – appropriate classification/reorganization of electronic records is necessary for future EDRMS / recordkeeping system implementation</li> <li>• Information related to and supporting business functions is fragmented – staff regularly experience difficulty locating records needed for their work or may not have access to the information they need</li> </ul>	High	<ul style="list-style-type: none"> <li>• Official BCER information is being inadequately managed – the problem is steadily increasing as more records are created and received.</li> <li>• Risks include:                             <ul style="list-style-type: none"> <li>– Inability to locate critical information</li> <li>– Non-compliance with applicable IM legislation, policy and best practices</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Strategy, Contracted Resource &amp; Funding (\$) for Ongoing Services:</b></li> <li>• Projects involve the classification and organization of electronic records in accordance with government's approved records schedule for such records.</li> </ul>	<ol style="list-style-type: none"> <li>1. Initiates a key foundational activity necessary for establishing a state of EDRMS readiness.</li> <li>2. Addresses sensitive records (personal information).</li> <li>3. Implementation activities will serve to test the suitability of classification</li> </ol>	Ongoing	RIM Contractor (Michelle Barroca)  With assistance from:  EDRMS Specialist BCER Branches IT/IS

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
					<ul style="list-style-type: none"> <li>- Destroying records before they are legally eligible for destruction (not keeping records long enough)</li> <li>- Keeping records longer than required; this can create risks associated with FOI and document production under litigation (e.g. having to produce records that legally could/should have been destroyed)</li> <li>- Mixing transitory information with official records</li> </ul>	<ul style="list-style-type: none"> <li>• Ongoing/systematic implementation of the ORCS on a program-by-program basis across the BCER.</li> <li>• Contract has been initiated with RIM consulting company (FY Information Management).</li> <li>• <b>Ongoing project – 19 branches successfully completed</b></li> </ul>	<ul style="list-style-type: none"> <li>structures (ARCS, ORCS or HRAS) and identify any scheduling gaps.</li> <li>4. Supports informed decision-making by Commission staff through making information accessible.</li> </ul>		
<b>BData Defragmentation Strategy - Digitization</b>									
3		<b>Addressing the Hardcopy Well Files and Well Data Fragmentation Problem:</b>  Creation of Data Source Roadmap to Identify Locations of Relevant Well Data/Records	<ul style="list-style-type: none"> <li>• <b>Update – should include the Field and Pool and Applications and Activities on the K drive</b></li> <li>• <b>Upload to eLibrary - currently they go to FTP – DK now naming and putting on K drive into Applications and Activities structure.</b></li> <li>• <b>Currently a person gets FTP data link for FSJ, and also an e_Library – easier for client and creates a full record.</b></li> <li>• Well data/records exist in multiple locations and formats throughout the Commission; onsite in FSJ (paper files); offsite in storage (Victoria); staff emails/Outlook; systems/databases; K: Drive; other shared drives.</li> <li>• The data/records are highly fragmented and inaccessible to staff (and public).</li> </ul> <p style="text-align: center;">s.13 / s.17</p>	High	s.13	<b>Create a Data Source Roadmap:</b> <ul style="list-style-type: none"> <li>• Create a reference tool to identify all "pieces" where Commission well data is located; this will assist staff with locating information, and support planning of future projects</li> <li>• Engage with other key staff within Planning &amp; Technology Division, who may be collecting similar data for related initiatives</li> </ul>	<ol style="list-style-type: none"> <li>1. Identifies/illustrates severity of current well data/records data fragmentation situation within Commission</li> <li>2. Information will serve as the basis for corporate business planning/working towards solutions</li> <li>3. Information sharing benefit - supports collaboration with other branches/key staff to ensure information accuracy/completeness</li> </ol>	Initiated	RIS Branch  FSJ Records/Permit Administration (Jody Sutherland)  <i>With input from:</i>  Planning & Technology Division (Strategic Initiatives, Business Intel)
4		<b>Addressing the Hardcopy Well Files and Well Data Fragmentation Problem:</b>  Conversion of Pre-2014 Records from Hardcopy to Electronic Format	<p><b>Background:</b></p> <ul style="list-style-type: none"> <li>• In 2014, the Commission introduced new requirements and technology (eSubmission) for permit holders to submit well records in electronic format only. This business process change ended receipt of well file records in paper format and helped to resolve a paper records backlog issue.</li> <li>• Some digitization of pre-2014 well file records has been completed; approximately 500 boxes out of a total 5000 boxes of well files</li> <li>• Presently, one FTE is dedicated to digitizing paper well records (Well File Technician).</li> </ul> <p><b>Issue 1: Legislative obligations under OGAA and Information Management Act (IMA) and the expectation of well data in digital format</b></p> <ul style="list-style-type: none"> <li>• Under OGAA, the Commission is required to provide well data (non confidential wells) to the public upon request.</li> <li>• All data is requested in electronic format by internal and external clients.</li> <li>• New information management legislation in BC (IMA) will require government information be created and maintained in digital format only (exceptions to digitization requirements may be made on a case-by-case basis).</li> </ul> <p><b>Issue 2: High volume of requests received for pre-2014 well data in electronic format – Slow response time to public requests</b></p> <ul style="list-style-type: none"> <li>• The Commission converted to digital well submissions in 2014 (eSubmission); well data received prior to 2014 was predominantly received in paper format with some electronic data provided on CDs, diskettes.</li> <li>• <b>FSJ office supports onsite scanning by the public;</b> Victoria does not – all external requests for pre-2014 well data requires in house</li> </ul>	High	<ul style="list-style-type: none"> <li>• Defining corporate direction and a long term strategy for digitization will support appropriate planning, budgeting, resourcing and prioritization of supporting projects and activities.</li> <li>• Well file records are made available in digital format to external and internal requestors; paper is no longer the format of choice. The majority of the Commission's well data exists in paper format (approximately 4500 out of 5000 boxes of records have not yet been made digitally available).</li> <li>• Well records are severely fragmented – documentation is filed in separate files and geographical locations (e.g. PST records, well logs, etc.). The only way to efficiently integrate/combine the records is through electronic means. Interfiling "paper" is not a feasible option based on how the records are currently maintained.</li> <li>• BC's new legislation (IMA) may require the Commission to digitize its records over time, due to their FR (full retention) assessment by a provincial archivist. With such an assessment, the records will be permanently maintained by BC Archives. BC Archives is developing a digital archives for government records – in future, only records in electronic format will be accepted for permanent transfer from government to the Archives. Although the Commission will retain the majority of its</li> </ul>	<p style="text-align: center;">s.13 / s.17</p> <p>Option 1</p> <p style="text-align: center;">s.13 / s.17</p>	<ol style="list-style-type: none"> <li>1. Establishes corporate direction and long-term vision for the Commission's management and publication of well data</li> <li>2. Supports a digital environment and better access to information</li> <li>3. Resolves current file integrity and OGAA compliance issues: (i) well file records are scattered across multiple locations; (ii) files deemed 'masters' are actually incomplete (missing key records); (iii) the Commission is not providing complete information to the public for decision-making purposes.</li> <li>4. Supports intent of the new IMA that government records be created/received "digitally"</li> <li>5.</li> <li>6. Digitization positions the Commission to be able to destroy paper versions of records once a digital version of the file</li> </ol> <p style="text-align: center;">s.13 / s.17</p>	Ongoing	Well File Technician  s.13 / s.17

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
			<p>scanning. As noted above, scanning requests are managed by one FTE (Well File Technician).</p> <ul style="list-style-type: none"> <li>The volume of well data requests is high and multiple requests are received weekly.</li> <li>In addition to external requests from industry, RIS branch routinely responds to monthly ministry requests (land sale audit) and ad hoc internal requests (orphan site audits).</li> <li>Public expectation is that the Commission will provide requested data quickly; this expectation, coupled with the fact that there is only one FTE providing the service, puts considerable and constant pressure on that one FTE.</li> </ul> <p><b>Issue 3: Well data is fragmented throughout the Commission –</b></p> <p>s.13 / s.17</p> <p><b>Issue 4: The eLibrary is being publicly advertised as the official source for Commission well data</b></p> <ul style="list-style-type: none"> <li>The eLibrary is described on the Commission's external website as the digital archive for oil and gas data.</li> <li>Commission staff direct the public to the eLibrary as the Commission's official repository of electronic well file data.</li> <li>To date, the eLibrary only includes the contents of the well files originating in Victoria; it does not include the contents of FSJ's hardcopy well files. For additional information, please refer to Issue Number 16.</li> </ul> <p><b>Issue 5: An ad hoc approach to well file digitization</b></p> <ul style="list-style-type: none"> <li>There has been no master digitization 'plan' applied to the scanning of Commission records.</li> <li>Digitization is typically done in an ad hoc manner, in response to internal and external requests for specified well data. The requests 'drive' which records are selected for scanning.</li> <li>When the Victoria office move was announced, effort was made to digitize the files that were stored in the onsite file room; approximately 50% were digitized before the move.</li> <li>Only 10% of the Commission's total paper well files (Victoria files) have been converted to digital format to date (500 out of a total 5000 boxes of files).</li> <li>When requests for older records are received, the files are retrieved from storage, converted to digital format, and uploaded into eLibrary.</li> <li>Commission well data is fragmented; it is located in multiple formats and locations. For additional information, please refer to Issue Numbers 11 through 14.</li> </ul> <p><b>Issue 6: Long-term offsite storage of well file records is costly over time</b></p> <ul style="list-style-type: none"> <li>There are approximately 5000 boxes of well files stored in Victoria offsite records storage facilities.</li> <li>Cost for storage is \$.56/box per month = \$34,800 per year</li> </ul>		<p>records for a long period of time, some will eventually be eligible for transfer.</p> <ul style="list-style-type: none"> <li>The Commission should have a plan for addressing the digitization requirement for well files that will meet legal requirements, and support their accessibility and long term preservation</li> </ul>	<p><b>Option 2:</b> Outsource well file scanning to an external service provider through a multi-year service agreement.</p> <p>s.13 / s.17</p> <p><b>Option 3:</b> A combined approach that incorporates Options 1 &amp; 2.</p> <p>s.13 / s.17</p> <p><b>Summary of Items For Decision:</b></p> <ol style="list-style-type: none"> <li><b>Determine Which Files Should be Digitized:</b> <ul style="list-style-type: none"> <li>(a) Digitize all well files over time;</li> <li>(b) Digitize select well files; or</li> <li>(c) Digitize well files upon request (status quo).</li> </ul> </li> <li><b>Determine How Digitization Should Be Addressed:</b> <ul style="list-style-type: none"> <li>(a) Use internal resources;</li> <li>(b) Outsource to contracted service provider; or</li> <li>(c) A combined approach of (a) and (b).</li> </ul> </li> </ol>	<p>has been created – this would be subject to:</p> <ul style="list-style-type: none"> <li>An approved ORCS authorizing the destruction</li> <li>Ensuring the IT environment appropriately safeguards the digital records and supports their permanent preservation (e.g. upon implementation of an EDRMS)</li> <li>Government digitization and Commission quality standards for the records have been met</li> </ul> <p>7. Systematic destruction of the hardcopy well files, once digitized, would reduce the Commission's ongoing, long-term box storage costs:</p> <ul style="list-style-type: none"> <li>Storage of 5000 boxes of well files costs <u>\$34,800 per year</u></li> <li>Storage of 700 boxes of well logs costs <u>\$4,870 per year</u></li> <li>Total annual storage cost is <u>\$39,670 per year</u></li> </ul>		

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

3

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
5		<p><b>Addressing the Commission's Hardcopy Well Files and Well Data Fragmentation Problem:</b></p> <p>Risk of Legislative Non-Compliance:</p> <p><u>Well Log Records</u></p> <p>Commission may not be releasing complete information on wells to the public</p> <p>Relates to need for long-term strategy to address well file digitization (Issue Number 10)</p>	<ul style="list-style-type: none"> <li>Storage cost (assuming rates remain unchanged at \$0.58 per box per month) to store these records boxes for another 25 years would cost the Commission approximately \$991,750, as these records have a long-term retention requirement.</li> <li>Under the ORCS, well file records are fully retained (essentially kept "forever", until the Commission no longer requires them).</li> <li>The Commission is required to make specified well data publicly available under the OGAA General Regulation.</li> <li>There are approximately 700 boxes of well logs stored at Iron Mountain records storage in Vancouver, BC; these records should be filed within the corresponding well file, but are not.</li> <li>The logs were previously removed from FSJ's hardcopy well files due to onsite storage limitations (space-saving measure).</li> <li>While it's possible that a significant percentage of these logs are duplicates of those contained within Victoria's hardcopy well files, this is unknown and cannot be verified unless a comparison is done: (1) to the paper log to the well file contents; or (2) to the digital logs that have been uploaded to eLibrary.</li> <li>The box content lists that were completed identify the logs by a well authorization (WA) number. It's possible to retrieve the logs related to a specific WA; it is not possible, however, to determine from the lists the exact number of logs related to a specific WA.</li> <li>The Commission (RIS Branch) previously initiated discussions for a potential digitization contract with a Vancouver-based scanning service provider (MicroCom Systems) for 150 boxes of well logs, however this contract did not proceed. Proceeding with any scanning contract is not recommended until a strategy has been determined – ideally, the separated logs should be compared against the file contents of the "master" well files to identify/destroy any duplicates prior to initiating scanning.</li> </ul> <p>s.13 / s.17</p> <p>(at the time MEMPR had the well files, and logs weren't used up in FSJ)</p>	Med-High	<ul style="list-style-type: none"> <li><b>Incomplete files:</b> If the logs are not duplicates of those currently filed within the corporate well files, it means a portion of Victoria's WA files are missing relevant data and therefore "incomplete" (data integrity issue).</li> <li><b>Incomplete responses:</b> This translates into an information request compliance issue, in that the Commission may not be releasing complete records in response to external requests, nor publishing complete WA data on eLibrary. The public is routinely directed to the eLibrary as the Commission's "official" well file data repository.</li> <li><b>Non-compliance with OGAA General Regulation:</b> In terms of requested information, this omission could put us in contravention of OGAA General Regulation (the Commission's requirement to make well data available to the public). Unlike the FSJ office, Victoria is not set up for public access/self-scanning – this means that the public relies on the Commission to fully satisfy requests for well data.</li> <li><b>Ongoing cost for storage:</b> Based on the current rate of \$0.58 per box per month, the annual storage cost for the 700 boxes of logs is approximately \$4,870. It's estimated that the logs have been in offsite storage for approximately 7 years, hence \$34,000 has been spent to date on storing what could be duplicate records.</li> </ul>	<p>s.13 / s.17</p> <p>Initiate log reconciliation/digitization project after substantial amount (e.g. 40-50%) of well files have been digitized. The logs are believed to pertain to more historical (older) well files that have not yet been digitized. The RIS Branch has not yet digitized many of the historical files; focus has been directed more on recent files (those that were physically stored in the Victoria Records Centre).</p> <ul style="list-style-type: none"> <li>At some point, the hardcopy logs need to be reconciled against the well files to determine what is an original versus a copy, or if the log is missing altogether.</li> <li>This comparison is best done against logs that are digitized and available in electronic format (within eLibrary); a "paper" to electronic comparison approach would be taken.</li> <li>When a significant portion of the Commission's historical well files have been digitized and uploaded to eLibrary, the hardcopy logs could then be retrieved from storage and compared to the electronic versions. This work would be completed by the Victoria Well File Technician.</li> <li>Duplicate logs would be destroyed. Logs missing from the uploaded data would be digitized and added.</li> <li>The amended ORCS, once approved, will provide legal authority for the destruction of the paper well files (including logs) once digitized.</li> </ul> <p>s.13 / s.17</p> <p><b>Funding (\$)</b> for External Scanning Services:</p> <ul style="list-style-type: none"> <li>Addressing these records through a digitization project is the recommended approach for resolving this issue – converting records from paper to electronic format will make them accessible to Commission staff and the public. It will also support our goal of trying to unify the records that pertain to each well.</li> <li>Once the Commission's amended ORCS has received provincial approval, the Commission will be authorized to destroy the paper records once they've been digitized (subject to Executive approval)</li> <li>This would be an appropriate project to outsource to a contracted service.</li> </ul>	<ol style="list-style-type: none"> <li>Addresses OGAA compliance issue</li> <li>Addresses record format, accessibility, data fragmentation, and duplication issues</li> <li>Supports the eventual reduction of offsite records storage costs over time</li> <li>Supports Commission's move towards a digital records environment</li> </ol>	On Hold	<p>No resource to support</p> <p>s.13/s.17</p>
12		<p><b>Addressing the Hardcopy Well Files and Well Data Fragmentation Problem:</b></p> <p>Risk of Legislative Non-Compliance:</p> <p><u>Pressure Test Records</u></p> <p>Commission may not be releasing complete information on wells to the public</p> <p>Relates to need for long-term strategy to address well file digitization (Issue Number 10)</p>	<ul style="list-style-type: none"> <li>There are approximately 128 boxes of hardcopy Pressure Test documents currently located in offsite storage.</li> <li>These documents were formerly filed within Field &amp; Pool files when the records belonged to the Ministry; a retroactive decision was later made by the Commission to have the document files in the well files. Document re-filing work was never completed by the Commission.</li> <li>The issue is that this data is now stored separately and not part of the official well file; as a result, the data is not available to Commission staff or the public in response to information requests.</li> <li>The boxes of records in storage are listed by Field &amp; Pool/Project type. With the current arrangement of the records, it would be a difficult, multi-step process to try to locate and retrieve Pressure Test documents related to a specific well.</li> </ul>	Med-High	<p>s.13 / s.17</p> <ul style="list-style-type: none"> <li>This finding relates and contributes to the problem of the Commission's fragmented well data (file integrity issues); files regarded as "master" files by the Commission are incomplete and missing key documents.</li> <li>It is not feasible to refile the paper documents into the master well files – a single box of Pressure Test records contains documents related to 100 or more well files. The hardcopy well files are all maintained in offsite storage –</li> </ul>	<p><b>Funding (\$)</b> for External Scanning Services:</p> <ul style="list-style-type: none"> <li>Addressing these records through a digitization project is the recommended approach for resolving this issue – converting records from paper to electronic format will make them accessible to Commission staff and the public. It will also support our goal of trying to unify the records that pertain to each well.</li> <li>Once the Commission's amended ORCS has received provincial approval, the Commission will be authorized to destroy the paper records once they've been digitized (subject to Executive approval)</li> <li>This would be an appropriate project to outsource to a contracted service.</li> </ul>	<ol style="list-style-type: none"> <li>Addresses OGAA compliance issue</li> <li>Addresses record format, accessibility, data fragmentation issues</li> <li>Supports the eventual reduction of offsite records storage costs over time</li> <li>Supports Commission's move towards a digital records environment</li> </ol>	s.13/s.17	Records Analyst

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

4

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
					refiling would require the storage company to retrieve 100 or so different boxes of well files for <u>every one box</u> of Pressure Test documents. Refiling would need to be done onsite at the storage facility; the Commission would need to provide a resource to work onsite.	<u>provider such as BC Mail Plus</u> , as the documents are originals and of a regular/standard size (8 1/2 x 11). BC Mail Plus is able to retrieve specified boxes directly from storage, scan their contents, and manage the destruction process.			
13	DONE	<u>Addressing the Commission's Hardcopy Well Files and Well Data Fragmentation Problem:</u>  Risk of Legislative Non-Compliance: <u>Oil, Gas &amp; Water Analysis Records</u>  Commission may not be releasing complete information on wells to the public  Relates to need for long-term strategy to address well file digitization (Issue Number 10)	<ul style="list-style-type: none"> <li>There are approximately <u>21 boxes</u> of hardcopy Oil, Gas &amp; Water Analysis documents currently located in offsite storage.</li> <li>These documents should have been previously filed into the applicable Well files – it's possible that the documents were either removed from the master files and never refiled, or never filed into the master files upon their receipt by the Ministry or Commission (e.g. the Commission may have "inherited" the problem).</li> <li>The issue is that this data is not part of the official well file and, as a result, not being made available to Commission staff or the public in information requests.</li> <li>As the boxes of records are inadequately listed, it is almost impossible to locate/retrieve analysis documents related to a specific well.</li> </ul>	Med-High	<ul style="list-style-type: none"> <li>Same as above - This finding relates and contributes to the problem of the Commission's fragmented well data (file integrity issues); files regarded as "master" files by the Commission are incomplete and missing key documents.</li> <li>Risks include: the Commission not meeting statutory obligations related to the release of well data; and, Commission staff, researchers, etc. not having access to all pertinent information for decision-making.</li> </ul>	<ul style="list-style-type: none"> <li>Same as above - Addressing these records through a digitization project is the recommended approach for resolving this issue – converting records from paper to electronic format will make them accessible to Commission staff and the public. It will also support our goal of trying to unify the records that pertains to each well.</li> <li>Once the Commission's amended ORCS has received provincial approval, the Commission will be authorized to destroy the paper records once they've been digitized (subject to Executive approval)</li> <li>This would be an appropriate project to outsource to a contracted service provider such as BC Mail Plus, as the documents are originals and of a regular/standard size (8 1/2 x 11). BC Mail Plus is able to retrieve specified boxes directly from storage, scan their contents, and manage the destruction process</li> </ul>	<ol style="list-style-type: none"> <li>Addresses OGAA compliance issue</li> <li>Addresses record format, accessibility, data fragmentation issues</li> <li>Supports the eventual reduction of offsite records storage costs over time</li> <li>Supports Commission's move towards a digital records environment</li> </ol>	Completed in December 2021	Records Analyst
14		<u>Addressing Well Data Fragmentation - Records stored in Email/Staff Outlook Systems:</u>  <u>Well Exemption Records</u>  Critical emails that document evidence of Commission exemption decisions are not accessible to key decision-makers	<ul style="list-style-type: none"> <li>Engineering and Permit Administration/Adjudication staff require knowledge of any exemptions granted to operators</li> <li>These records are not stored in a centralized location or system – most are stored within the Outlook (email) systems of individual staff</li> <li>These records should be included as part of the Commission's activity files (well, facility, pipeline) in a centralized and shared location</li> <li>Lack of access to these records has negatively impacted Commission business (e.g. compliance, investigation and enforcement activities)</li> </ul>	High	<ul style="list-style-type: none"> <li>Key staff require knowledge of access to exemption decisions to effectively do their work</li> <li>Lack of access can (and has) result in the Commission making incorrect assessments or decisions, and/or being put in a position of "embarrassment" (e.g. there have been cases where the Commission was unaware of an exemption when dealing with an operator)</li> </ul>	<ul style="list-style-type: none"> <li>Collaborative Project with IT/IS (Possible Technical Solution) and Permit Administration (Possible Resource/Project Assistance):</li> <li>Work with IT/IS to identify</li> </ul> <p style="text-align: center;">s.13 / s.17</p>	<ol style="list-style-type: none"> <li>Addresses OGAA compliance issue</li> <li>Addresses record accessibility, data fragmentation issues</li> <li>Supports informed business decisions</li> </ol>	Initiated	<p><i>** Preliminary discussion with IT/IS has occurred re identifying/testing possible technological approaches or solutions</i></p> <p><i>Process changed – engineering now uploading themselves. 800+ docs digitized and uploaded. Completed – October 2023</i></p> <p>Potential for assistance/ assignment to FSJ Resource Data Coordinator staff</p>
15		<u>Conversion of Hardcopy Field &amp; Pool Files to Electronic Format</u>	<ul style="list-style-type: none"> <li>The Field &amp; Pool files are another key records series currently maintained in hardcopy format.</li> <li>The files were previously stored in onsite office space (Victoria Records Centre), but have since been boxed and moved to offsite</li> </ul>	Medium	As noted, continuation of a paper filing system will be problematic for a number of reasons: <ul style="list-style-type: none"> <li>Files will have to be continuously retrieved from storage in order to do filing</li> </ul>	<b>Dedicated Project Resource (RIS Branch Records Analyst):</b>	<ol style="list-style-type: none"> <li>Digitization supports staff accessibility to information (Engineering &amp; Geology) and proactive release, as appropriate</li> </ol>	In Progress	Records Analyst  With assistance from:

**Commented (TS1):** Correct number of boxes is 10. The box number range is #11-21. Accession number 95-2703. In process of scanning & uploading to eLibrary.

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).



Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
		Digitizing Key Record Series Maintained/Utilized by Reservoir Engineering & Geology Staff	<p>storage. Ongoing filing of paper documents will be required as long as no digital file version exists – paper filing can no longer be sustained in the current environment as it would require ongoing retrieval of records boxes from storage. There is no room for file expansion within the 94 boxes of records, nor will the storage facility support retrieving records for an ongoing 'active' filing system.</p> <p>In addition to the 94 boxes, there are an additional 100 or more boxes of older Field &amp; Pool records in offsite storage.</p> <p>A Project Charter was developed for a Field &amp; Pool record digitization project by RIS Branch with Reservoir Engineering approximately 2-3 years ago. RIS Branch is now fulfilling that former commitment.</p> <p><b>Priorities are done – no asks for remaining offsite material. There is still work to be done but the critical elements are done and operational work is supported.</b></p> <p>Update – ST and MF</p>		<ul style="list-style-type: none"> <li>Inter-filing into 'boxes' is difficult and will eventually lead to the need to re-box records as more documentation gets added to the files (limited expansion capabilities)</li> <li>Technically we are not supposed to store 'active' records in offsite storage – frequent retrievals may result in offsite storage facility raising this issue</li> <li>BC Government is going digital – as well as the Commission; an ongoing 'print and file' approach is not sustainable or in alignment with the direction of records management.</li> <li>Longer term vision is to make some of the Field &amp; Pool information publicly available (e.g. via eLibrary)</li> </ul>	<ul style="list-style-type: none"> <li>In collaboration with program staff, RIS Branch established a new electronic filing structure on the K: drive for Field &amp; Pool records (to support the digital transition to records management)</li> <li>Project focus is on the 94 boxes of records that were previously stored in the Victoria Records Centre; boxes are being retrieved from offsite storage incrementally and file contents digitized. Approved naming conventions are being applied to scanned records, and records are being organized in accordance with the new e-filing structure. The records meet naming convention standards required for future uploading to IRIS/eLibrary</li> <li>The Analyst is analyzing file contents in detail and addressing any noted file integrity issues.</li> <li>Regular updates and engagement with the Reservoir Engineering team is occurring ensure input into project.</li> <li>RIS Branch will assess the value/need of digitizing the older Field &amp; Pool files located in storage in future; conversion to digital format may or may not be warranted.</li> </ul>	<ol style="list-style-type: none"> <li>Digitization supports a necessary program area shift to accept only 'digital' record submissions</li> <li>Once ORCS Phase 1 is approved, the Commission will be authorized to destroy the scanned/duplicate paper copies (reduces offsite storage costs)</li> <li>The process is supporting necessary corrections at a file and document level, thus improving file quality and integrity (e.g. opportunity to address misfiled documents)</li> </ol>		EDRMS Specialist Reservoir Eng Geology
<b>File Integrity</b>									
16		<p><u>External Release/Publication of Well Information:</u></p> <p>Appropriate Management of the Two Sets of Well Files Maintained by Victoria and FSJ Offices</p> <p>Relates to need for long-term strategy to address well file digitization (Item Number 10)</p>	<ul style="list-style-type: none"> <li>Two sets of hardcopy well files exist within the Commission. One set is located in Victoria (offsite storage), and the other in FSJ (File Room). There are different document types filed within these sets. Victoria's files include records related to pre-drilling and drilling data, whereas FSJ's files include records related to post-drilling activities.</li> <li>When individuals request a copy of a well file, the type of records received is often dependent on the office to which the request is made.</li> <li>A request that is received by/directed to the Well File Technician results in a release of records from the Victoria well file – records found in the 'sister' well file in FSJ are typically not included as part of the response (unless the WA file cannot be located in Victoria, or specific documents related to the FSJ file are requested). Likewise, requests/walk-ins to the FSJ office result in different records being provided to the public.</li> <li>FSJ office supports public walk-ins and onsite scanning of well files by the public. Victoria does not support walk-ins for onsite file viewing; rather, requests are managed internally by the RIS Branch (Well File Technician) who retrieves the requested well files from offsite storage, scans the records, and uploads the information to eLibrary. The requester completes the registration process to obtain a user ID for access to online viewing within eLibrary.</li> <li>Not all records filed in the FSJ well files are releasable under FOIPPA (e.g. Londoner and First Nations information is confidential).</li> <li>Files are partially duplicated – Victoria is the "technical file" and FSJ the "field" file, but when FSJ received the only copy of a "completion report" they kept it so they do have some technical material that Victoria doesn't have.</li> </ul>	Medium	<ul style="list-style-type: none"> <li>Different records are available for release to the public based on office location.</li> <li>Only records found in the Victoria well files are currently published on eLibrary – as previously noted, eLibrary is often pointed to as the only "source" of records for a given well.</li> <li>Some members of the public may not be aware of the two sets of files and difference between their contents.</li> <li>OGAA General Regulation identifies the types of well data that should be available for release. The Commission also has a requirement to make information available for viewing or copying. This is being done by the two office locations for the files they have custody of/access to, but it is not necessarily being done as a 'coordinated' activity.</li> </ul>	<p><b>Further Assessment Required:</b></p> <ul style="list-style-type: none"> <li>Review and compare contents of the FSJ and Victoria well files; create a "document" inventory to understand the differences.</li> <li>Review statutory requirements of OGAA in terms of release.</li> <li>Flag documents not subject to release under FOIPPA.</li> <li>Review current business processes maintained within and between the two offices with respect to managing information requests.</li> <li>Determine whether or not any of the records maintained in the FSJ files should be included with well data made available in eLibrary; if yes, think about possible strategy/business process to support need.</li> <li>Solution may include enhancements to current technological platforms/systems, such as AIMS, IRIS/Kemint, eSubmission, to support document uploading.</li> </ul>	<ol style="list-style-type: none"> <li>Improves RIS Branch understanding of Commission well file records and current records management processes</li> <li>May identify service gaps and/or confirm OGAA compliance issue</li> </ol>	Pending	RIS Branch  Permit & Administration
<b>Administrative Efficiency</b>									
18		<p><u>Classification of Unscheduled Hardcopy Records in Storage:</u></p> <p>Portion of Records in Offsite Storage Require Classification/Scheduling According to</p>	<ul style="list-style-type: none"> <li>Some records have been sent to offsite storage without being unclassified/unscheduled, as "miscellaneous ARCS &amp; ORCS".</li> <li>Others have not had final disposition applied.</li> <li>This work will require time and analysis.</li> <li><b>Some analysis – planned.</b></li> </ul>	Low-Med	<ul style="list-style-type: none"> <li>The Commission may be holding onto records and paying for records to remain in storage longer than necessary</li> <li>Records held in storage are subject to FOI and litigation</li> </ul>	<p><b>Hold Until ORCS Development Phase 1 is Approved &amp; RIM Project Priorities Established for 2019/20:</b></p> <ul style="list-style-type: none"> <li>As time and resources permits, review offsite record 'holds' and box content lists to identify those unscheduled; complete</li> </ul>	<ol style="list-style-type: none"> <li>Supports records lifecycle management</li> <li>Potentially reduces scope of FOI or litigation related requirements</li> <li>Could reduce offsite storage costs</li> </ol>	On Hold	No resource to support  RIS Branch resources busy with other high priority projects

Original draft – 2018. In the process of being updated, FY 2024/25. Red font first start at updates, greyed lines completed items – remove as we work through the sheet (and renumber lines).

6

Issue Number	Priority Ranking	Issue	Issue Background or Description	Risk Rating	Activity Significance / Risks if Not Completed	Recommended Solution	Benefit to Commission	Status	Current Resource(s)
		ARCS/ORCS to Support Application of Final Disposition				necessary steps to have retention applied so that final disposition can occur <ul style="list-style-type: none"> <li>Focus on 'quick wins'; identify/flag accessions that may require more in depth analysis and time to address</li> </ul>			
19		<u>Improvement of Tools for Managing Offsite Records Holding</u>  Current Tools for Managing/Locating Corporate Offsite Record Holdings are Inadequate	<ul style="list-style-type: none"> <li>Multiple versions of excel tracking spreadsheets are maintained by the records management staff for locating records.</li> <li>RIS Branch staff face a complicated, multi-step process for searching, locating and retrieving records from offsite storage.</li> <li>Data in Kermit is not entirely reliable in terms of the location of records – staff try to update when they come across inaccurate information.</li> </ul>	Medium	<ul style="list-style-type: none"> <li>It is difficult for RIS Branch staff to do basic record searches and retrievals from storage with confidence – this is a risk when responsive records must be produced within rigid time limits for FOI or litigation.</li> <li>There is heavy reliance on one staff (Records Analyst) to interpret data contained within the multiple spreadsheets and locate records.</li> </ul>	<b>Funding (\$)</b> For External Services - Option of Small Dollar Contract to Complete Work in 2019/20: <ul style="list-style-type: none"> <li>Branch would highly benefit from development of a simple/searchable database (e.g. Access database) that amalgamates/contains all key information related to the Commission's offsite record holdings</li> </ul>	<ol style="list-style-type: none"> <li>Addresses record accessibility, data fragmentation issues</li> <li>Reduces risk of non-compliance associated with records searches</li> </ol>	On Hold	Records Analyst IST Sr Bus Analyst  With assistance from: Well Tech

**New items from brainstorming/review session:**

Disposition of Shared Drive FD Folders

SharePoint Projects

Scanner wearing out – Terri

Cancelled wells – boxed in numeric order, possibly 120 boxes, there is a spreadsheet of all of them by WA number. Mixed up files that are cancelled but also with land disturbance so land disturbance needs to go on the shelf. Cancelled need documented destruction.

Waste Management Files – organized and put into order.

Space out the shelves better in FSJ Records Centre.

DRAFT

ISSUANCE: Corporate Services Division  
Finance & Administration Department

APPROVED: August 10, 2018

## 1.0 GENERAL

### 1.1 Purpose

The BC Oil and Gas Commission (Commission) views information as an important and strategic asset that must be appropriately managed throughout its lifecycle according to legislated requirements. This policy details the roles, responsibilities and principles for the effective and compliant management of Commission records.

### 1.2 Background

The Commission is subject to the statutory requirements of the *Information Management Act* (IMA) which requires the digitization of non-digital records (subject to specific exemptions) and the use of appropriate information management systems.

### 1.3 Applicability

This policy applies to all records, regardless of format, that are created or received by the Commission and its employees in the course of their duties. It also applies to contractors, consultants and agents of the Commission who have access, custody or control of Commission records.

### 1.4 Authority

- *Information Management Act*
- *Interpretation Act*
- *Electronic Transactions Act*
- *Oil and Gas Activities Act*

### 1.5 Definitions

- **Active records** are records referred to frequently for daily business operations, or that need to be retained and easily accessible on site (if records exist in physical format).
- **Administrative records** support common organizational functions such as the management of facilities, property, finance, personnel, and information systems. These records are managed (classified and scheduled) in accordance with the government Administrative Records Classification System (ARCS).
- **Confidential records** contain information requiring protection against unauthorized access or disclosure. Records are classified as confidential based on a variety of requirements, including, but not limited to, policy or legislation. For example, the *Freedom of Information and Protection of Privacy Act* (FOIPPA) identifies exceptions to the disclosure of requested information. Examples of Commission confidential records include well data, where confidentiality periods apply as defined in the drilling and production regulations, and First Nations

consultations and draft agreements.

- **Digital (electronic) records** consist of information that is entered, created, manipulated and/or stored on digital media or storage devices, and includes:
  - Records that are born digital;
  - Digitized records (converted from non-digital format);
  - Unstructured data (e.g. documents); and
  - Structured data maintained within electronic systems.
- **Electronic Document and Records Management System (EDRMS)** is an integrated software system capable of managing both electronic and physical records through their life cycle in accordance with ARCS, ORCS and other approved records schedules.
- **Inactive records** are no longer required for ongoing business. These are records that are ready for final disposition or, in other words, records for which the scheduled active and semi-active retention periods have lapsed.
- **Information management** is the systematic control of information from creation to storage and retrieval to dissemination, regardless of media or physical format.
- **Operational records** relate to those mandated functions which are unique to a government public body, for which it is responsible for performing according to statute, regulation or policy. These records are described in an Operational Records Classification System (ORCS).
- **Records** include any recorded information created or received, and retained in the day to day operations of business. This covers “books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise” as defined in the *Interpretation Act*.
- **Recordkeeping system** within a government office refers to a shared ARCS and ORCS based filing system in which official (non-transitory) records are organized, retained and disposed of according to approved record retention schedules. A recordkeeping system may consist of physical files in a file room, electronic folders and records saved on a shared drive, or an Electronic Document and Records Management System (EDRMS).
- **Retention schedule** provides a timetable for maintaining an organization’s records. It governs the life cycle of a file from creation, through active use to inactive storage (when appropriate) to final destruction or their transfer to the custody and control of the Provincial Archives. The approved retention schedules for government records are defined in ARCS and ORCS and are applied throughout a records life cycle.
- **Semi-active records** are used only occasionally and do not need to be maintained in the office space of the Commission. While they still have value, they can be stored in economical, offsite storage facilities.
- **Transitory records** are records of temporary usefulness that are not an integral part of an administrative or operational record series. Transitory records are not required to meet statutory obligations or to sustain administrative or operational

functions. As with all records, they can exist in any format or medium (paper or electronic). These records are not regularly filed with official Commission records within filing systems.

## **2.0 PRINCIPLES OF INFORMATION MANAGEMENT**

The Commission must manage its digital (electronic) and physical (hardcopy) records in accordance with legislated requirements and government-wide policies and standards for recordkeeping.

### **2.1 Access to Records**

Records are a corporate asset and resource, and need to be accessible and shared by staff where appropriate. Access to sensitive or confidential records will be restricted to individuals whose duties require such access, in adherence with applicable information security classifications.

### **2.2 Duty to Document**

Employees must create and maintain complete and accurate records sufficient to document evidence of their business activities, transactions, policy or decisions.

### **2.3 Digital (Electronic) Records**

Records created or received in digital (electronic) format shall be treated as the authoritative records source and remain in digital (electronic) format. As both the Commission and BC government move to a digital recordkeeping environment, printing and filing records in hardcopy should be avoided where feasible. Physical records may be digitized and stored electronically as the authoritative source, provided government's digital conversion standards are met. Destruction of any physical records after their digitization must be approved and documented by the Commission's records management staff.

### **2.4 Recordkeeping**

Program areas are responsible for maintaining a shared office recordkeeping system for official active records. Records form corporate memory and must be incorporated into the shared recordkeeping system upon creation or as soon as practical. Government legislation requires the filing and retention of records in accordance with approved government records classification and retention schedules.

### **2.5 Records Disposition**

When records reach their inactive stage they are ready for final disposition review. Records management staff will carry out the review and determine whether records require further retention or disposal. Commission records are not to be destroyed or disposed of without approval from the designated Corporate Records Officer.

### **2.6 Records Storage**

When records become semi-active they will be moved into the applicable records storage facility (physical records) or managed within a secure records environment (electronic records) as determined by the Corporate Records Officer or prescribed in the Commission's records management procedures.

### 3.0 RESPONSIBILITIES

#### 3.1 **Executive and management are responsible for:**

- Cultivating an organization-wide culture that values records and information management;
- Enforcing policy and procedures for the proper collection, creation, storage, access, retention and disposal of information; and
- Ensuring proper levels of protection are applied to confidential information under their custody and or control.

#### 3.2 **Each employee is responsible for:**

- Managing their records in accordance with appropriate records retention schedules, policies, procedures and best practices;
- Understanding, identifying and routinely disposing of transitory information created or received; and
- Protecting records in their custody or under their control from unauthorized disclosure, inadvertent loss or destruction.

#### 3.3 **Commission records management staff are responsible for:**

- Delivering an efficient and effective Records Management Program that offers succinct processes, solutions, and records management strategies;
- Providing Commission-wide records retention schedule(s), data plans, policies, procedures and guidelines related to collection, creation, storage, access, retention and disposal of records;
- Assessing organizational training and resource support needs, and developing appropriate plans and materials to address these;
- Assisting in defining records management business requirements and integrating information management planning into systems, plans and budgets and;
- The approval of and secure disposal of records.

**APPROVAL:**




---

**Paul Jeakins**  
Commissioner,  
Chief Executive Officer




---

**Len Dawes**  
Executive Vice President,  
Chief Financial Officer




---

**Ken Paulson**  
Executive Vice President,  
Chief Operating Officer




---

**Mayka Kennedy**  
Executive Vice President,  
Chief Engineer




---

**Trevor Swan**  
Executive Vice President,  
Chief Legal and Regulatory Officer

**Version Control:**

Document Created	Aug-18	



## Information Security Policy

### Information Technology

ARC 100-00/200

Issuance: Corporate Services Division

**Approved by Executive February 15, 2017**

## GENERAL

The OGC is the custodian of extensive information holdings and relies upon its information assets for fiscal, policy and program delivery initiatives. The management of public information requires government agencies to protect confidentiality, integrity and availability of the information assets in its care.

The Information Security Policy is based on the ISO 27002:2005 standard for information security management and conforms to the spirit of Chapter 12 of the Core Policy and Procedures manual. This standard provides a structured approach to identifying the broad spectrum of information security activities in the life-cycle of information systems. This Information Security Policy provides the framework necessary for the protection of Commission information and technology assets.

The policy incorporates a risk assessment approach to security by considering, business process and government service delivery implications and technological implications.

The risk assessment approach enables:

- Compliance with legislative and policy objectives;
- Cost-effective allocation of resources based on a risk assessment;
- Responsible governance of the Commission's information assets; and,
- Secure provision of electronic services.

The Information Security Policy includes a Glossary of key terms. Terms from existing policies are adopted where appropriate.



## **Introduction**

### **Chapter 1 - Security Policy**

### **Chapter 2 - Organizing Information Security**

### **Chapter 3 - Asset Management**

### **Chapter 4 - Human Resources Security**

### **Chapter 5 - Physical and Environmental Security**

### **Chapter 6 – Information Security Services**

### **Chapter 7 - Access Control**

### **Chapter 8 - Information Systems Development and Maintenance**

### **Chapter 9 - Information Security Incident Management**

### **Chapter 10 - Disaster Recovery & Business Continuity Management**

### **Chapter 11 - Compliance**

## **Glossary**

## Chapter 1 - Security Policy

The Information Security Policy establishes requirements to ensure that information security policies, processes and practices remain current as business needs evolve and technology changes.

The Senior Network Security Analyst is responsible for establishing, issuing and monitoring information security policies.

### 1.1 - Information Security Policy

#### a) Information Security Policy

The Information Security Policy (ISP) contains operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of Commission services. Secure service delivery requires the assurance of confidentiality, integrity, availability and privacy of Commission information assets through:

- Management and business processes that include and enable security processes;
- Ongoing personnel awareness of security issues;
- Physical security requirements for information systems;
- Governance processes for information technology;
- Reporting information security events and weaknesses;
- Creating and maintaining Disaster Recovery plans; and,
- Monitoring for compliance.

#### b) Compliance with BC CIO Information Security Policy

This policy follows and enhances the BC Government ISP. The Commission ISP can exceed but must not conflict with the baseline established by the BC Government Office of the Chief Information Officer's Information Security Policy.

### 1.2 - ISP Annual Review and Updating

#### a) Information Security Policy review

The Senior Network Security Analyst is responsible for reviewing information security policies, standards and guidelines on an annual basis. Policies and standards review must be initiated:

- In conjunction with legislative, regulatory or policy changes which have information management implications;
- During planning and implementation of new or significantly changed technology;
- Following a Security Threat and Risk Assessment of major initiatives (e.g., new information systems or contracting arrangements);
- When audit reports or security risk and controls reviews identify high risk exposures involving information systems;

## 1.2 - ISP Annual Review and Updating cont.

- If threat or vulnerability trends produced from automated monitoring processes indicate the probability of significantly increased risk;
- After receiving the final report of investigation into information security incidents;
- Prior to renewing third party access agreements which involve major government programs or services;
- When industry, national or international standards for information security are introduced or significantly revised to address emerging business and technology issues; and,
- When associated external agencies (e.g., Information and Privacy Commissioner, National CIO Sub-Committee on Information Protection, RCMP) issue reports or identify emerging trends related to information security.

## Chapter 2 - Organizing Information Security

This chapter describes the management structure needed to coordinate information security activities including who coordinates them and what agreements are required. This coordination applies to Commission employees and to external parties accessing or managing the Commission's information assets.

The Commission Information Systems & Technology (IST) Department requires the support of a network of contacts in the information security community to elicit advice, trends and to deal with other external factors.

### 2.1 - Internal Organization

#### a) Executive commitment to information security

Executive must set direction and provide support for information security by:

- Ensuring that information security reviews and audits are supported;
- Assisting business units when conducting security threat and risk assessments;
- Approving reasonable capital and operating expenses necessary to provide adequate information security for the Commission;
- Employing a dedicated information security specialist;
- Identifying and reporting significant threat changes and exposures to threats of assets associated with information security;
- Supporting the IST department in their implementation of security controls, training and awareness.

#### b) Information security specialist responsibilities

Planning and implementation of information security activities across the Commission must be coordinated by the Senior Network Security Analyst by:

- Interpreting the Information Security Policy to assist in the delivery of business functions;
- Evaluating information security implications of new Commission initiatives;
- Performing information system security risk analysis activities;
- Performing information security assessments and reviews;
- Evaluating new threats and vulnerabilities;
- Investigating information security incidents;
- Advising on the information security requirements for documented agreements with third party service providers;
- Identifying general business trends and emerging technologies, and recommending changes to Information Security staff training;
- Analyzing and providing advice on emerging information security standards; and,
- Providing information security advice for business areas.

### **c) Information Owners**

Information Owners are Commission staff who have the responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure and working with the IT department will:

- Determine business requirements including information security needs;
- Ensure information and information systems are protected commensurate with their information classification and value;
- Define security requirements during the planning stage of any new or significantly changed information system;
- Determine authorization requirements for access to information and information systems;
- Approve access privileges for each user or set of users;
- Document information exchange agreements;
- Develop service level agreements for information systems under their custody or control;
- Implement processes to ensure users are aware of their security responsibilities;
- Monitor that users are fulfilling their security responsibilities; and,
- Be involved with security reviews and/or audits.

### **d) Confidentiality agreements**

Confidentiality agreements reflecting organizational requirements for the handling of information must be in place and reviewed regularly by contract owners (contractor managers) and the Specialist of Procurement & Internal Policy.

Information Owners must:

- Ensure employees are informed of their obligation to maintain the confidentiality of information; and,
- Ensure individuals other than employees accept and sign an agreement to maintain the confidentiality of information.

Confidentiality requirements must be reviewed and updated annually.

### **e) Contact with service providers**

Appropriate contacts shall be maintained with service providers of information technology and services including but not limited to:

- Internet service providers;
- Vendors of security and monitoring software or appliances in use at the Commission;
- Internal network service providers (including firewalls and network intrusion protection services).

**f) Information Technology Department staff**

Personnel with information security responsibilities must maintain their knowledge of information security industry trends, best practices, new technologies and threats or vulnerabilities by:

- Participating in information exchange forums regarding best practices, industry standards development, new technologies, threats, vulnerabilities, early notice of potential attacks, and advisories;
- Maintaining and improving knowledge regarding information security best practices; and,
- Creating a support network of other security specialists.

**g) Approval for information systems**

Information Custodians of a new or significantly modified information system must, with the assistance of the IT department:

- Conduct a Security Threat and Risk Assessment;
- Address security requirements in the development of the system;
- Conduct a risk and controls review to determine if controls are adequate to mitigate business risks prior to implementation of the information system; and,

Prior to acquisition of new hardware, firmware or software, Information Custodians must consult with the IT Department to:

- Evaluate compatibility with existing information systems hardware, firmware and software;
- Ensure new hardware, firmware and software conform to the Information Security Policy, standards and guidelines;
- Consider the reliability of the product as part of the procurement selection process; and,
- Evaluate the need for any additional security measures and the impact on existing security processes.

Personnel must not store Commission information on non-Commission hardware, off-site storage, web or cloud services unless authorized by the IT department. The IT department must test non-Commission systems for vulnerabilities prior to utilizing the hardware or service.

**2.2 - External Parties**

**a) Risk assessment related to external parties**

Assessment of risks from external party access to Commission information or information systems must be undertaken and appropriate security controls implemented.

Information Owners are responsible for assessing the business requirements and associated risks related to external party access to information and information systems.

Risk assessments must be documented during the conceptual design phase of a project and updated throughout the lifecycle of the information system (e.g., prior to and following technical or business process changes to the information system).

The assessment of risks related to external party access must consider:

- If existing controls prevent external parties from accessing facilities or information that are not needed to meet the business requirements for the access,
- Impacts to the controls of the information processing facilities involved,
- The classification of the information assets,
- Policies and processes the external party has for personnel hiring, training (on security and privacy issues) and incident reporting,
- Internal and external processes for managing and reporting security and privacy incidents,
- Processes for identifying, authorizing, authenticating and reviewing access rights of personnel and systems of the external party,
- Security controls to be used by the external party when storing, processing, communicating, sharing or exchanging information,
- Impacts to both parties resulting from assets being unavailable, and,
- Data integrity requirements including impacts of accessing or using inaccurate information.

Prior to authorizing access by external parties to information and information systems Information Owners must confirm that:

- A risk and controls review has been completed and identified risks have been mitigated or accepted;
- The terms and conditions of access are documented (e.g. services agreements, contracts, memoranda of understanding);
- Responsibilities for managing and monitoring the external party access have been assigned and documented; and,
- Security controls have been implemented and tested.

#### **b) Addressing security when dealing with external parties**

Identified security requirements must be addressed prior to granting external parties access to information, information systems or information processing facilities.

Prior to authorizing access by external parties to information and information systems Information Owners must confirm that:

- A risk and controls review has been completed and identified risks have been mitigated or accepted;
- The terms and conditions of access are documented (e.g. services agreements, contracts, memoranda of understanding);
- Responsibilities for managing and monitoring the external party access have been assigned and documented; and,
- Security controls have been implemented and tested.

### **c) Addressing security in external party agreements**

Arrangements involving external party access to information, information systems or information processing facilities must be based on a formal contract containing necessary security requirements.

Information Owners must ensure access to information assets and information processing facilities by external parties is only provided after an access agreement has been completed.

Access agreements must include:

- Roles and responsibilities of the Information Owner, Information Custodian and the external party;
- Approved security controls;
- Conditions for contract termination;
- Audit and compliance monitoring rights, responsibilities and processes;
- Reporting obligations for suspected or actual security and privacy incidents;
- Renewal and extension conditions; and,
- Requirements for regular compliance reviews.

Approved forms of agreement include:

- General Service Agreement for purchase of goods or services;
- Agreements for Alternate Service Delivery or Public Private Partnership;
- Information Sharing Agreement; or,
- Other forms of agreement as approved by Legal Services.

Information Owners must ensure the security requirements of external party access agreements include:

- Notification of obligations of the parties to adhere to legislation and regulation;
- Requirements to adhere to agreed information security policies and procedures;
- Processes for amending the agreement;
- Acknowledgement by the external party that ownership of information is retained by the Commission;
- Confidentiality obligations of the external party and their personnel or agents;
- Requirements for use of unique user identifiers;
- Processes for conducting audits and compliance monitoring activities;
- Responsibilities and processes for reporting security and privacy incidents; and,
- Assurances that disciplinary action will be applied to employees or contractors who fail to comply with the terms of the agreement.



## Chapter 3 - Asset Management

Information and information systems services constitute valuable Commission resources. The asset management chapter establishes the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

To account for the assets that require protection, this chapter specifies the requirement to designate who owns assets. Designated owners become responsible for protecting information and technology assets and to maintain the way assets are protected.

This chapter sets the foundation for a system that classifies information to identify different security levels, to specify how much protection is expected and how information should be handled at each level. Not all the information requires the same level of protection because only some information is sensitive or confidential.

### 3.1 - Responsibility for assets

There is a need to identify and manage information and information technology assets associated with information systems or services ("assets") to provide control and accountability, support strategic planning, enhance critical incident response, system planning, protection, maintenance and recovery.

#### a) Identification of assets

Information Custodians must identify assets under their control including:

- Software;
- Hardware;
- Services including computer and communications services, and general utilities;
- Information assets required to be inventoried in the personal information directory (required under the Freedom of Information and Protection of Privacy Act); and,
- All other information assets including: database and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information.

#### b) Documenting and maintaining asset inventories

The Information Custodians must document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of the Commission risk management strategy.

Information Owners with the assistance of Information Custodians must document, maintain and verify information assets

The following information should be recorded to facilitate system planning and asset recovery in the case of interruption, corruption, loss or destruction:

- Type of asset;
- Ownership;
- Format;
- Location;
- Back-up information and location;
- License information;
- Sensitivity and safeguards requirements;
- Criticality for service delivery and maintaining business functions;
- Consequences of loss.

**c) Loss, theft or misappropriation of assets.**

The loss, theft or misappropriation of assets must be reported. Where the loss, theft or misappropriation involves information the Information Owner and IT Department must be immediately notified. Where the loss, theft or misappropriation involves hardware (computers, phones, portable media, etc.) the IT department must be immediately notified.

### 3.2 - Designating Information Owners/Custodians

Information Owners and Custodians must be designated for all assets associated with information systems.

**a) Responsibilities for Information Owners**

An Information Owner is responsible for controlling the production, development, maintenance, use and security of information assets within their jurisdiction. Information Owners are responsible for:

- Working with the IT Department to ensure the appropriate safeguarding of information and technology systems or services;
- Defining and regularly reviewing access restrictions and safeguards of their designated information; and,
- Bringing any information security concerns to the immediate attention of the IT Department.

**b) Responsibilities of the IT Department**

The IT Department is the Custodian of all information and technology systems or services within the Commission and is responsible for:

- Overseeing the functioning of information and technology assets;
- End-to-end security of information assets;
- Delivery of services in accordance with defined service requirements; and,
- Regular reporting on designated information and technology assets.

### 3.3 - Acceptable use of Commission resources

Rules for the acceptable use of information systems must be identified, documented and implemented to help prevent misuse or compromise of Commission information systems.

**a) Acceptable use of Commission resources**

All users of the Commission's information systems must take responsibility for, and accept the duty to actively protect the Commission's information and technology assets. Expectations for the use of Commission information systems are described in the *Usage of IT Resources Policy*. Compliance with the usage policy is critical in securing Commission information assets.

The requirements for personal use of Commission information systems are described in the *Usage of IT Resources Policy*.

### 3.4 - Information classification

The Commission does not employ a formal information security classification system. Information owners must take into account the value, sensitivity and intended use of the information when creating and reviewing access restrictions for:

- Internally shared files;
- IS systems (financial records, well records, etc);
- Files accessible by the public or third parties (FTP, websites, etc.); and,
- Email or other electronic communications.

**a) Information handling/transmission procedures**

Information deemed sensitive or confidential must only be transmitted via an encrypted method. These methods include:

- Encrypted USB storage provided by the IT department;
- SSL web connection with minimum TLS 1.0 and 256 bit keys;
- TLS FTPS transfer; and,
- Internal SMB file transfers.

Information deemed sensitive or confidential must also have an authentication method prior to providing access.

**b) Information storage procedures**

Storage of information assets has the following requirements:

- All information is stored with the assumption it is confidential;
- Portable devices and systems (including phones, laptops, USB media) must be encrypted;
- Files shares and not local laptop drives are used to store information with the exception of local email profiles and caches.
- The IT Department is responsible for all hardware related to the storage of information at the Commission.

## Chapter 4 - Human Resources Security

This chapter identifies the information security requirements for personnel that have an employment relationship with the Commission. To reduce information security risks, the terms and conditions of employment must establish expectations for the protection of Commission assets, information and services.

This chapter references the terms and conditions set by the Commission for employees and identifies the conditions for external personnel such as contractors or volunteers

Management and personnel have different security responsibilities and liabilities that apply prior to, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of the expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies establish management responsibilities, education, training and formal processes to handle problematic security situations. This chapter also establishes rules to ensure a secure transition when employment is ended or has changed.

### 4.1 - Prior to employment

#### a) Security roles and responsibilities

Information Owners must:

- Document information security roles and responsibilities for personnel in job descriptions, standing offers, contracts, and information use agreements; and,
- Review and update information security roles and responsibilities when conducting staffing or contracting activities.

#### b) Communication of security roles and responsibilities

Managers must ensure personnel are informed of their security roles and responsibilities by establishing processes for communicating security roles and responsibilities to protect information system assets.

### 4.2 - Personnel screening must be performed prior to employment

#### a) Personnel screening

Personnel should be screened to assess their: education, skills, knowledge, experience, and past work performance. The screening should also confirm the applicant's identity.

The extent of the screening process should be commensurate with the sensitivity of the information (identified by the information owners) and nature of work to be performed.

**This screening applies to future staff, contractors or volunteers.**

### **b) Criminal records screening**

HROD, on the recommendation of the hiring manager, will designate positions requiring criminal records checks. The Commissioner must approve all designated positions. Positions with the following primary functions must be designated:

- Positions having access to sensitive information. Sensitive information can be about employees, clients or others and may be held by the Commission is any information that, if compromised, could result in serious consequences for individuals, organizations, or the Commission.
- Positions with expense/budget authority and/or revenue authority in excess of \$500,000.
- Positions responsible for Commissions corporate safety and/or security.
- Positions responsible for and who have unrestricted access to operational, data and information management systems where the disruptions of such a system could significantly impact services or reveal confidential information.
- Senior leadership and executive positions

## **4.3 - During employment**

### **a) Management responsibilities**

Management must ensure personnel comply with security policies and procedures. Managers must support the implementation of information security policies and practices by:

- Ensuring personnel are informed of information security roles and responsibilities prior to being granted access to information or information systems;
- encourage staff to participate in IT department sponsored information security training;
- Ensuring personnel to adhere to information security policies and are duly informed that any breach of security rights may include discipline up to and including termination;
- Reviewing and validating security roles and responsibilities in all job descriptions, standing offers, contracts and information use agreements on an ongoing basis.

## **4.4 - Information security training and awareness of security policy**

Personal awareness and education of security threats, risks and concerns and information security policies and procedures are required for all Commission staff to help protect the Commission against electronic threats.

### **a) Orientation for new personnel**

The IT Department is responsible for designing, developing and delivering an information security awareness orientation processes that all personnel (regular, contract, volunteer) must complete prior to being granted access to any electronic information systems.

The IT department must ensure there is a specific/separate training module for all managers and supervisors to ensure roles and responsibilities and non-compliance consequences are clearly understood.

### **b) Ongoing information security awareness, education and training**

The IT Department must provide at a minimum of once per year ongoing information security awareness, education and training, addressing topics including but not limited to:

- Protection of information;
- Known information security threats;
- Legal responsibilities;
- Information security policies and directives;
- Procedures for reporting information security events to the IT Department;
- Appropriate use of Commission resources;
- How to obtain security advice;
- File storage and transmission security for Information Owners; and,
- Application management (email, Service Desk, etc.).

## **4.5 - Security breaches and policy violations**

### **a) Reviewing security breaches and policy violations**

Upon receipt of information identifying personnel responsible for a security breach or policy violation, managers and Information Owners are responsible for:

- Ensuring the IT and HROD Departments are notified immediately of the potential security breach or policy violation;
- Assisting in an investigation and verifying the details of the security breach or policy violation;
- Determining, in consultation with the HR Department, if disciplinary action is warranted for employees;
- Determining if disciplinary action is warranted for non-employees; and,
- Arranging for permanent or temporary removal of access privileges when appropriate.

Upon receipt of information identifying personnel responsible for a security breach or policy violation, the IT Department will follow a security breach process (Information Incident Management Process).

## **4.6 - Termination or change of employment**

### **a) Termination of employment**

Managers must advise outgoing personnel of ongoing confidentiality responsibilities that continue to apply after termination of employment as per the Employee Code of Conduct and Ethics policy.

### **b) Return of assets**

Managers must document the return of Commission assets in the possession of personnel upon termination of their employment. Return of assets includes:

- documents, files, data, books and manuals in physical or other media formats including other information assets developed or prepared by an employee or contractor in the course of their duties,
- computer hardware, software and equipment (e.g., mobile devices, portable media), and access devices, cards, vouchers and keys (e.g., credit cards, taxi cards, travel vouchers);
- Returned items are verified against established asset inventories;
- Recovery or compensation for assets not returned, based on established criteria regarding depreciation and replacement value for classes of items; and,
- Identification of unreturned access devices, cards and keys that could permit unauthorized access or alteration/destruction of assets, so that information and/or security systems can be protected.

### **c) Reduction of access rights**

The access rights of personnel to information systems must be removed upon termination of employment and reviewed upon change of employment.

Managers must review access to information systems and information processing facilities when personnel change employment, including:

- When personnel assume new roles and responsibilities;
- During restructuring of positional or organizational roles and responsibilities;
- When personnel commence long-term leave; and,
- Updating directories, documentation and systems.

Managers must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment status by contacting the IT Department, Corporate Property Department and also the IS Department if the employee had access to IS systems (Kermit, IRIS, AMS, etc). This contact should be in the form of a Service Desk employee exit at least one week prior to exit.

The IT and IS departments are responsible for removing access from files and systems by midnight of the employee exit or by the specific time mentioned by the manager if the time of day is to be earlier than midnight.

Corporate Property department is responsible for receiving all physical access keys and cards by the time the employee leaves the premises on his/her last day.

## Chapter 5 - Physical and Environmental Security

This chapter identifies requirements for the protection from environmental and man-made threats to personnel and property in information processing facilities. One of the principles used for protection is the use of security zones to place computers and information in secure areas. Safety measures for equipment installations are also described.

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the confidentiality, integrity and availability of Commission information and information systems.

### 5.1 - Secure areas

Commission information processing facilities must be protected by a physical security perimeter to prevent unauthorized physical access.

#### a) Security perimeter

All information processing facilities are a Restricted Access Security Zone.

Appropriate security controls must be applied to reduce the level of identified risks and include:

- A structure that prevents external visual and audio observations and complies with all local building codes for structural stability (external walls, internal walls, ceilings and doors).
- Appropriate access control mechanisms must be applied to prevent unauthorized access;
- All information processing facilities must be equipped with physical intrusion alarm systems that automatically alert monitoring staff to take immediate action;
- Access to restricted zones must be controlled, authorized and monitored as required by the applicable zone;
- Commission information processing facilities must be physically separated from those managed by third parties.
- Escorting visitors;
- Securing sensitive or valuable information and assets when leaving the work areas; and,
- Taking precautions when discussing sensitive information.

#### b) Entry controls

Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Access to any Commission information processing facility or areas where sensitive information is kept must be restricted. These rules must be followed when accessing server rooms and wiring closets:

- Only IT personnel have access to these areas;
- Visitors must be accompanied by IT personnel;
- Personnel must challenge anyone in a secure area who is not accompanied by IT personnel;
- Visitors must sign in and obtain temporary access badges from reception.
- Visitor or temporary access badges must be returned and accounted for at the end of each day;
- Access rights to secure areas must be reviewed and updated regularly.

#### c) Physical security requirements



Physical security requirements must be designed, documented and applied for all areas in and around an information processing facility.

The IT department must design, document and approve security controls for information processing facilities. Considerations must include:

- Determining security perimeter and maintenance factors;
- Establishing appropriate security zones;
- Design and construction complying with health and safety regulations and standards;
- Selecting unobtrusive sites and keep signage to the minimum required for meeting fire and other safety requirements;
- Limiting the identification of information processing facility locations, in publicly and internally available directories, to the minimum required; and,
- Selecting sites so that public access can be strictly controlled or avoided.

**d) Other secure area requirements**

- Activities within a secure area are confidential and must not be discussed in a non-secure area, or with persons who do not have a need-to-know;
- Sensitive information must not be discussed with persons without a need-to-know; and,
- Maintenance staff and cleaners need not have unescorted access to secure areas.

## 5.2 – Site considerations

**a) Design and site selection**

Physical security controls must be designed to protect against damage from natural or man-made disaster.

The IT Department and site planners (Corporate Property Administration) must incorporate physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster. Consideration must be given to any security threats presented by neighbouring premises or streets. In addition to meeting building code specifications and fire regulations:

- Combustible or hazardous materials must be stored at a safe distance from the secure area. Bulk supplies must not be stored within the secure area;
- Installing camera monitoring systems;
- Installing fire alarm and fire suppression systems;
- Installing humidity sensors and alarms;
- Installing temperature sensors and alarms;
- Uninterruptible power supply, back-up generators, and fuel, as required by business and technical requirements; and,
- Fallback equipment (e.g., for DRP) and backup media must be sited at a safe distance to avoid damage from a disaster affecting the main site.

### **b) Equipment location**

The IT department is responsible for ensuring that the design and layout of information processing facilities provides protection from security threats. Safeguards must include:

- Locating servers and other centralized computing equipment within a Restricted Access Security Zone;
- Protecting information processing equipment from observation by unauthorized persons, including by observing through windows and walking through work areas;
- Ensuring that kiosks and public terminal safeguards are in place.

### **c) Equipment protection**

The IT department is responsible for ensuring that the design and layout of information processing facilities provides protection from physical and environmental hazards. Safeguards must include:

- Ensuring that equipment is properly vented and that the temperatures and humidity in information processing facilities are appropriate for operating equipment safely;
- Providing lightning protection for information processing facilities which includes surge protection for power and communications;
- Assessing and protecting equipment to minimize damage from fire suppression and other safety systems;
- Protecting equipment from potential damage from environmental hazards such as water, dust, vibration, and sunlight;
- Ban eating and drinking in work areas containing equipment (other than personal computers);
- Briefing personnel who work with equipment about safety practices in the workplace;
- Keeping information processing facilities free of biological pests that pose hazards to equipment and power systems;
- Equipment, information or software belonging to the Commission must not be removed from premises without prior authorization; and,
- Regularly inspecting the information processing facility(s) for integrity of ceilings, walls, windows, and other infrastructure for damage from water and other environmental factors that may pose a threat to safe equipment operation.

### **d) Off-site equipment security controls**

Equipment must be protected when off-site from Commission sites to guard equipment from loss or unauthorized access.

The IT Department must ensure that Commission equipment being used off-site is protected, matching with the sensitivity of the information it contains and the value of the equipment. These controls must be in place:

- Portable computers are encrypted;
- Equipment is protected from unauthorized access by the use of a password;
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate;
- Personnel are familiar with operation of the protection technologies in use;
- Not leave Commission equipment unattended in a public place;

- Ensure that equipment is under their direct control at all times when travelling;
- Take measures to prevent viewing of sensitive information other than by authorized persons;
- Not permit other persons to use the equipment; and,
- Report loss of equipment immediately to the IT Department.

### 5.3 – Disposal or re-use of storage devices

#### a) Erasure or reassignment of hardware and media

Information, records and software must be protected against unauthorized disclosure when hardware and media are reassigned or destroyed.

The IT Department must consider the value and sensitivity of the information stored on hardware or media when determining whether it will be reassigned within the Commission, forensically wiped or destroyed.

Prior to reassignment of hardware or media within the Commission it must be ensured that:

- That the integrity of Commission records is maintained by adhering to Records Management policies;
- Information and software is erased using methods and standards approved by the Office of the Government Chief Information Officer; and,
- Asset inventories are updated to record details of the erasure and reassignment including:
  - Asset identifier,
  - Date of erasure or reassignment; and,
  - Names of personnel conducting the erasure or reassignment.

#### b) Destruction of hardware

The IT Department is responsible for ensuring hardware media used to store information or software is destroyed in a secure manner if forensic erasure is not possible.

## Chapter 6 – Information Security Services

This chapter establishes a framework to support the integration of information security in the services provided by the Commission information processing facilities.

Planning and management of the day-to-day activities is required to ensure the availability and capacity of the resources that provide services. This framework identifies requirements to control and monitor operations for service delivery and to manage changes as the operations evolve.

Controls for operations include documented processes, staff duties and formal methods to implement systems and changes. This includes:

- Methods to protect information;
- Create copies for back-up and to manage the retention schedules; and,
- Network protection requirements from threats such as viruses or unauthorized disclosure are also described.

### 6.1 – Security Documentation

#### a) Operations documentation

Operations documentation must contain detailed instructions regarding:

- Information processing and handling;
- System re-start and recovery;
- System testing after maintenance;
- Back-up and recovery, including on-site and off-site storage;
- Exceptions handling, including a log of exceptions;
- Output and media handling, including secure disposal or destruction;
- Audit and system log management;
- Change management including scheduled maintenance and interdependencies;
- Server room management and safety;
- Information Incident Management Process;
- Disaster recovery;
- Business continuity; and,
- Operations, technical, emergency and business contacts.

#### b) Information Risk

Information Owners with the assistance of the Information Custodians must document the risks associated with the information they control through these methods:

- Identifying the sensitivity and confidentiality of information;
- Assessing the potential business impact, including the security impact, of information loss or theft;
- Identifying information retention periods;
- Identifying test procedures for secure access to data to assist with checks after maintenance and changes;
- Assessing any information access monitoring requirements for sensitive data; and,
- Assessing current data backup and server snapshot schedules.

## 6.2 – Change Management

### a) Planning changes

Information Custodians must plan for changes by:

- Assessing the impact of the proposed changes on security;
- Identifying impacts to dependant services;
- Identifying the impact on agreements with business partners and third parties including information sharing agreements, Memoranda of Understanding, licensing and provision of services;
- Preparing change implementation plans that include testing and contingency plans in the event of problems;
- Obtaining approvals from affected Information Owners;
- Notifying in advance all affected parties; and,
- Training technical staff and operations staff if required.

### b) Implementing changes

Information Custodians must implement changes by:

- Notifying affected parties, including business partners and third parties;
- Minimizing impact to business parties or staff;
- Training users if required;
- Documenting and reviewing the documentation throughout the testing and implementation phases;
- Recording all pertinent details regarding the changes; and,
- Checking after the change has been performed that only the intended changes took place.

## 6.3 - Segregation of duties and systems

Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized modification or misuse of information systems.

### a) Segregation of duties

Information Owners and Information Custodians must reduce the risk of disruption of information systems by:

- Requiring complete and accurate documentation for every information system;
- Rotating job duties periodically to reduce the opportunity for single individuals to have sole control and oversight on key systems;
- Automating functions to reduce the reliance on human intervention for information systems;
- Requiring that individuals authorized to conduct sensitive operations do not audit those operations;
- Maintaining a role based access password database organized such that no single individual has sole access to a system;
- Requiring that individuals responsible for initiating an action are not also responsible for authorizing that action; and,
- Implementing information systems security controls to minimize opportunities for collusion.

### **b) Separation requirements for systems**

The goal is to reduce the risk of unauthorized or inadvertent changes to operational information systems or information systems under development or being tested. Development and test information systems must be separated from operational information systems.

Information Custodians must protect operational information systems by:

- Separating operational environments from test and development environments using different servers (virtual or physical), storage partitions and networks if required;
- Preventing the use of test and development identities and credentials for operational information systems;
- Storing source code (or equivalent) in a secure location away from the operational environment and restricting access to specified personnel;
- Preventing access to compilers, editors and other tools from operational information systems;
- Using approved change management processes for promoting software from development/test to operational information systems;
- Limiting the use of personal information in development, test or training information systems.

## **6.4 – External Services**

### **a) External service delivery management**

Prior to using external information and technology services - security controls, service definitions and delivery levels must be identified and included in the agreement with the external party.

Information Owners and Information Custodians must include security requirements in procurement documents for information and information system services being delivered by external parties. Security requirements must be documented when:

- Drafting procurement documents (e.g., Request for Information, Request for Proposal);
- Evaluating bids to confirm acknowledgement and capability;
- Preparing agreements or contracts; and,
- Developing transition and fall back plans (e.g., migration from one service provider to another).

### **b) Service level continuity**

Information Custodians must ensure service agreements with external parties document service level continuity requirements and include processes for:

- Ongoing review of service level needs with business process owners;
- Audit and compliance monitoring rights and responsibilities;
- Communicating requirements to service providers;
- Obtaining periodic confirmation from service providers that adequate capacity is maintained; and,
- Reviewing the adequacy of the service provider's contingency plans for responding to disasters or major service failures.

Commission personnel managing external service delivery must regularly monitor and review services, reports and records provided by external parties and carry out regular audits.

### **c) Monitoring and review of external party services**

The Commission must regularly monitor and review services, reports and records provided by external parties and carry out regular audits to ensure compliance with security policies.

Information Custodians must establish processes to manage and review the information security of external party delivered services by:

- Assigning responsibility for monitoring to a designated staff member;
- Ensuring audit provisions are included in service delivery contracts;
- Maintaining an inventory of agreements and associated access rights;
- Monitoring for compliance through processes such as:
  - Conducting internal self-assessments of control processes,
  - Requiring external parties to submit annual management assertions that controls are being adhered to,
  - Conducting independent security reviews, audits and updates to risk and controls reviews, and,
  - Establishing a process, jointly with the service provider, to monitor, evaluate, investigate and remediate incidents.
- Establishing performance measures to ensure adequate service levels are maintained and measured.

### **d) Change management processes for external party services**

Change management must provide assurance that changes to information system services delivered by external parties maintain or enhance security controls.

Information Custodians must ensure agreements with external party service providers include provisions for:

- Amending agreements when required by changes to legislation, regulation, business requirements, policy or service delivery; and,
- Requiring the service provider to obtain pre-approval for significant changes involving:
  - Network services,
  - New technologies,
  - Use of new or enhanced system components (e.g., software or hardware),
  - System development, test tools and facilities,
  - Modification or relocation of the physical facilities, and,
  - Sub-contracted services.

Information Custodians must ensure the change management process for information systems services delivered by external parties includes, as required:

- Reviewing and updating the Security Threat and Risk Assessment to determine impacts on security controls;
- Implementing new or enhanced security controls where identified by the risk assessment;
- Initiating and implementing revisions to policies and procedures; and,
- Revising personnel awareness and training programs.

## 6.5 - System planning and acceptance

The use of information system resources must be monitored, optimized and projections made of future capacity requirements to reduce the risk of system failures and unacceptable performance levels.

### a) Resource capacity management

Information Custodians are responsible for implementing capacity management processes by:

- Documenting capacity requirements and capacity planning processes,
- Including capacity requirements in service agreements;
- Monitoring and optimizing information systems to detect impending capacity limits; and,
- Projecting future capacity requirements based on:
  - New business and information systems requirements,
  - Statistical or historical capacity requirement information, and,
  - Current and expected trends in information processing capabilities (e.g., introduction of more efficient hardware or software).

### b) Resource capacity planning

Information Custodians must use trend information from the capacity management process to identify and remediate potential bottlenecks that present a threat to system security or services.

### c) System acceptance process

Information Owners must ensure that system acceptance criteria are defined as part of the system development and acquisition process to ensure that new or upgraded information systems are tested against defined, agreed and documented criteria for acceptance, prior to becoming operational.

Prior to implementing new or upgraded information systems, Information Custodians must ensure:

- System acceptance criteria are identified including privacy, security and systems development; and,
- Security controls are accepted by the Senior Network Security Analyst.

### d) System acceptance criteria

Information Custodians must document system acceptance criteria, including:

- Projected performance and resource capacity requirements;
- Disaster recovery, restart, and contingency plans and procedures;
- Impact on standardized routine operating procedures and manual procedures;
- Implementation of security controls;
- Assurance that installation of the new system will not adversely affect existing systems, particularly at peak processing times;
- Disaster Recovery arrangements;
- Training requirements; and,
- User acceptance testing.



**e) Security certification**

Information Custodians must receive assurance that a new or updated information system meets minimum security acceptance criteria.

Assurance should be obtained from the Senior Network Security Analyst who will conduct a security controls review which determines whether a system includes adequate controls to mitigate security risks. This process will also determine the effect of the new system on the overall security of Commission information systems.

**f) System accreditation**

Information Custodians must authorize the implementation of new or upgraded information systems based on the degree to which the acceptance criteria are satisfied.

## 6.6 - Protection against malicious and mobile code

Security awareness, prevention and detection controls must be utilized to protect information systems against malicious code.

**a) Prevention and detection controls**

Information Custodians must protect Commission information systems from malicious code (e.g., viruses, worms) by undertaking such activities as:

- Installing, updating and consistently using software (e.g., anti-virus or anti-spyware software) designed to scan for, detect and provide protection from malicious code;
- Prohibiting the use of unauthorized software;
- Checking files, including electronic mail attachments and file downloads for malicious code before use; and,
- Maintaining business continuity plans to recover from malicious code incidents.

The Senior Network Security Analyst must ensure processes are implemented to:

- Maintain a critical incident management plan to identify and respond to malicious code incidents; and,
- Maintain a register of specific malicious code countermeasures (e.g., blocked websites, blocked electronic mail attachment file types and blocked network ports) including a description, the rationale, the approval authority and the date applied.

**b) Active controls**

The Senior Network Security Analyst must ensure there are more proactive measures in place. These include:

- Intrusion detection system on the edge of network;
- Scanning for code exploits on servers and systems; and,
- Email pre-scanning that goes beyond malicious code definitions and scanning heuristics.

### **c) User awareness**

The Senior Network Security Analyst is responsible for developing a user awareness program which will include education on malicious code countermeasures.

The Senior Network Security Analyst is responsible for communicating technical advice and providing information and awareness activities regarding malicious code.

Mobile code must be restricted to the intended information system or environment. a) Mobile code categorization

### **d) Restrictions on mobile code**

Mobile code must be restricted to the intended information system or environment.

To protect information systems from malicious mobile code these rules must be followed:

- Obtain digitally signed mobile code from trusted sources;
- Method implemented for blocking receipt or execution of mobile code;
- Use configuration controls to resist known exploits; and,
- Users should not access websites where the certificate is invalid.

## **6.7 - Back-up**

Information and information systems must be backed up and the recovery process tested regularly to enable the timely recovery of information and information systems.

### **a) Defining requirements**

Information Custodians with input from Information Owners must define and document backup and recovery processes that reflect the security classification and availability requirements of information and information systems including:

- Confirming that the backup and recovery strategy complies with:
  - Business continuity plans,
  - Policy, legislative, regulatory and other legal obligations, and,
  - Records management requirements, including the Administrative Records Classification System (ARCS) and Operational Records Classification System (ORCS); and,
- Documenting the backup and recovery processes including:
  - Types of information to be backed up,
  - Schedules for the backup of information and information systems,
  - Backup storage management (e.g., retention period, pattern of backup cycles),
  - Methods for performing, validating and labelling backups, and,
  - Methods for validating recovery of the information and information system.

### **b) Safeguarding backup facilities and storage**

Information Custodians must conduct a Security Threat and Risk Assessment to identify safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and information systems. Safeguards may include:

- Using encryption to protect the backed up information;
- Using digital signatures to protect the integrity of the information;
- Physical and environmental security;
- Access controls;
- Methods of transit to and from offsite locations (e.g., by authorized couriers, by encrypted electronic transfer);
- Storage of media adhering to manufacturer recommendations for storage conditions and maximum shelf-life; and,
- Remote storage of backup data at a sufficient distance to escape any damage from a disaster at the main site.

### **c) Testing**

Information Custodians must regularly test backup and recovery processes.

## **6.8 - Network security management**

A range of controls must be implemented to achieve and maintain security within the Commission network.

### **a) Control and management of networks**

Information Custodians must implement network infrastructure security controls and security management systems for networks to ensure the protection of information and attached information systems. The Senior Network Security Analyst is responsible for approving the design and implementation of these systems and controls.

Selection of controls must be based on a Security Threat and Risk Assessment, taking into account the information security classification determined by the Information Owners, and applicability to the network technology.

The Security Threat and Risk Assessment must consider network-related assets which require protection including:

- Information in transit;
- Stored information (e.g., cached content, temporary files);
- Network infrastructure;
- Network configuration information, including device configuration, access control definitions, routing information, passwords and cryptographic keys;
- Network management information;
- Network pathways and routes;
- Network resources such as bandwidth;
- Network security boundaries and perimeters; and,
- Information system interfaces to networks.

### **b) Configuration control**

To maintain the integrity of networks, Information Custodians must manage and control changes to network device configuration information such as configuration data, access control definitions, routing information and passwords.

Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of controls such as:

- Encryption;
- Access controls and multi-factor authentication;
- Monitoring of access;
- Configuration change logs;
- Configuration baselines protected by cryptographic checksums; and,
- Regular backups.

Status accounting must be regularly performed to ensure that configuration baselines reflect actual device configuration.

### **c) Secured path**

Where required by information classification, information must only be transmitted using a secured path.

Secured paths for information transmission must use controls such as data or session encryption, such as SSH, SSL or VPN tunnels.

### **d) Wireless Local Area Networking**

Wireless Local Area Networks must utilize the controls and must include:

- Strong link layer encryption, such as Wi-Fi Protected Access;
- User and device network access controlled by the IT Department;
- The use of strong, frequently changed, encryption keys and passwords or central authentication method like Radius;
- Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies; and,
- Port-based access control, for example use of 802.1x technology.

Where supported by information classification, additional controls for wireless networks may include:

- Virtual Private Network tunnel technology;
- The use of Desktop Terminal Services (DTS) technology; and,
- Intrusion detection systems, firewalls and Media Access Control (MAC) address filtering.

### **e) Equipment management**

Information Custodians must document responsibilities and procedures for operational management of network infrastructure, including devices at network boundaries and in user areas.

#### **f) Logging, monitoring and detection**

To facilitate monitoring, response and investigation, logging to a centralized log management service must be enabled, including logging of:

- Traffic traversing network security boundaries;
- Traffic within networks housing sensitive or mission critical systems or information;
- Security-relevant events on network devices, such as operator login and configuration changes; and,
- Security-relevant events on systems that provide authentication and authorization services to network infrastructure devices such as routers, firewalls or switches.

Logs must be continuously monitored to enable detection and response to security events and intrusions (e.g., automation of log monitoring and event alerting).

Active automated surveillance of networks must be implemented to detect and report on security events (e.g., network intrusion detection systems).

#### **g) Coordination and consistency of control implementation**

Information Custodians must document network security controls in the System Security Plan including:

- A summary of risks identified in the Security Threat and Risk Assessment;
- Roles and responsibilities for network security management;
- Specific procedures and standards used to mitigate risks and protect the network;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures (including monitoring frequency, review and remediation processes).

#### **h) Network service agreement**

Security features, service levels and management requirements of all network services must be documented and included in any network service agreement.

Formal network service agreements must be established between network service providers and consumers of network services to specify service levels, services offered, security requirements and security features of network services.

The network service agreement must include specification of:

- The rules of use to be followed by consumers to maintain the security of network services;
- The schedule for ongoing verification of network security controls;
- The rights of either party to monitor, audit or investigate as needed;
- Security incident response responsibilities, contacts and procedures; and,
- The requirement to meet or exceed Commission security policy and standards.

Information Custodians must confirm that the specified security features are implemented prior to commencement of service delivery.

## 6.9 - Media handling

All removable computer media must be managed with controls appropriate for confidential or sensitive data. Treating all data classifications the same will reduce human error

### a) Use of portable storage devices

The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and are easily lost, stolen or damaged, particularly when transported in public environments.

All portable storage devices must have whole disk encryption enabled by the IT Department before personnel can store Commission data on them. Only the IT Department can approve the type and make of a portable storage device.

Whenever possible, other data transmission methods should be used before information is stored on portable storage devices.

### b) Human factors

Information Custodians and Managers must ensure personnel using portable storage devices are:

- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with the encryption requirements;
- Familiar with operation of the required protection technologies and when they must not be used; and,
- Familiar with security event and loss reporting procedures.

### c) Risk assessment factors

The Security Threat and Risk Assessment must consider the impact of disclosure or loss of information stored on portable media from threats such as:

- Loss or physical theft;
- Limited ability to control and log access to stored data;
- Accidental media destruction;
- Improper long term storage environment;
- Exposure to malicious and mobile code; and,
- Incomplete erasure of data prior to device disposal.

Information classification and sensitivity levels must be considered in the risk assessment.

### d) Mandatory controls

Minimum information protection safeguards for the use of portable storage devices include:

- Disabling portable storage devices, media drives or connection ports where no business reason exists for their use;
- Treating all Commission data on portable storage devices as sensitive;
- Not storing the only version of a document on portable storage devices;

- Documented authorization processes for use of portable storage devices;
- Encryption of stored data;
- Contractual requirements for external parties that transport, handle or store portable storage devices;
- Prevention of mobile and malicious software,
- Logging of media custody and location to allow for:
  - Accounting and audit,
  - Media labelling to indicate owner,
  - Maintenance of information where the information storage requirement exceeds the expected media lifetime, and,
  - Secure erasure and disposal.

**e) Secure disposal of media**

Media must be disposed of securely and in a manner appropriate for the sensitivity of the data contained on the media.

Information Custodians must ensure that media that is no longer required operationally (e.g., due to expiry, surplus, damage or wear), is disposed of securely.

Media disposal procedures must:

- Be documented and communicated to personnel;
- Specify erasure and disposal measures whose strength is based on information sensitivity and type of media (e.g., erasure software);
- Include secure destruction of media if erasure is not sufficient, or not cost effective (e.g., destruction by shredding, incineration or chemical dissolution);
- Include secure storage measures for media collected for and awaiting erasure or disposal, to avoid undetected theft of small amounts of media from large volumes awaiting disposal; and,
- Include audit logs of media disposal.

**f) Media handling procedures**

Media must be handled and stored so as to prevent unauthorized information disclosure or misuse.

All removable computer media must be handled with controls appropriate for confidential or sensitive data.

The IT Department is responsible for media handling documentation which must include procedures for:

- Access control restrictions and authorization;
- Correct use of technology (e.g., encryption) to enforce access control;
- Copying and distribution of media, including minimization of multiple copies, marking of originals and distribution of copies;
- Operating the media storage environment and managing media lifespan according to manufacturer specifications;
- Regular status accounting of media;

- Maintenance of media transfer and storage records;
- Media destruction and disposal;
- User training; and,
- Use of non-Commission storage devices.

**g) Protection of systems documentation**

Information Custodians must ensure that documented procedures for the secure use and storage of systems documentation are established and followed. Procedures must:

- Require information classification labelling of system documentation;
- Establish lists of users authorized to access system documentation on a 'need to know' basis;
- Establish handling rules for the information regardless of storage media (e.g., electronic, paper);
- Require use of access controls, passwords, encryption or digital signatures as appropriate to the information classification; and,
- Include a compliance monitoring process.

**h) Electronic information exchange**

The Senior Network Security Analyst must document and implement procedures to protect information from interception, copying, misrouting and destruction when being transmitted electronically or verbally. Transmission methods include but are not limited to:

- E-mail, including attachments;
- Electronic file transfer (e.g., File Transfer Protocol (FTP), HTTPS transfers);
- Use of mobile devices;
- Telephone, cell, and other voice messaging;
- Faxes; and,
- Instant messaging.

## 6.10 – Exchanges of information

Information and software exchange agreements between the Commission and other organizations (including government) must be documented.

**a) Exchange agreements**

Information Custodians must ensure the terms and conditions for exchanging information assets with external parties is documented in an agreement. The agreement must define:

- Custody and control accountabilities;
- Authority of a custodian to publish, grant access to or redistribute the information;
- Purpose and authorized uses of the information or software;
- Limitations on data linkage;
- Duration, renewal and termination provisions;
- Primary contacts, for agreement, governance and management;



- Requirements for:
  - Protecting information according to its security classification,
  - Handling information (e.g., recording authorised recipients, confirming receipt of transmitted data, periodically reviewing records of authorised recipients),
  - Labelling information (e.g., methods to be used to apply and recognize labelling),
  - Maintaining integrity and non-repudiation of information, and,
  - Media management and destruction;
- Technical standards for transmission, recording or reading information or software;
- Responsibilities for reporting privacy and security incidents and breaches;
- Liability, accountability and mitigation strategies, for attempted, suspected or actual privacy and security incidents and breaches; and,
- Problem resolution and escalation processes.

#### **b) Information and software exchange requirements**

Information Custodians must ensure the following are completed for the information or software covered by the exchange agreement:

- An approved Privacy Impact Assessment; and,
- A Security Threat and Risk Assessment.

Exchange agreements must be reviewed by legal counsel for the Province prior to being signed.

#### **c) Media transport procedures**

Media being physically transported must be appropriately protected to protect information from unauthorized disclosure or loss.

Minimum media transport requirements are:

- Using couriers that are approved by government;
- Inspecting identification credentials of couriers upon pickup and delivery of packages;
- Obtain and retain receipts for media shipments;
- Using packaging that will protect the media from loss or damage;
- Packaging so that the sensitivity of the media is not displayed and the package is discreet; and,
- Using notifications of transport activities, such as:
  - Sender informing receiver of the impending shipment, and,
  - Receiver confirming receipt of the shipment;

Information transmitted by electronic messaging must be appropriately protected. a) General requirements

#### **d) Electronic messaging services**

Information transmitted by electronic messaging must be appropriately protected.

Electronic messaging services must be managed to protect the integrity of Commission messages by:

- Protecting messages from unauthorized access, modification or denial of service;
- Ensuring correct addressing and transportation of messages;

- Providing reliable and available messaging infrastructure; and,
- Conforming to legislative, regulatory and policy requirements.

The Senior Network Security Analyst must approve implementation of, and significant modification to, electronic messaging systems.

Personnel must support the responsible use of electronic messaging services by:

- Using only Commission electronic messaging systems;
- Using only authorized encryption for e-mail or attachments; and
- Not automatically forwarding Commission e-mail to external e-mail addresses;

Electronic messages created, compiled on, sent or received on Commission information systems are records of the Commission. These records:

- Are the property of the Government of British Columbia;
- Must be managed in accordance with the Document Disposal Act and the policies, standards and procedures in the Recorded Information Management Manual; and,
- Are subject to the access and the protection of privacy provisions of the Freedom of Information and Protection of Privacy Act.

#### **e) Information in business information systems**

Security controls must be implemented to mitigate the business and security risks associated with the interconnection of business information systems.

Information Custodians must document and implement procedures to restrict access to information in interconnected internal administrative and productivity information systems that support the Commission such as e-mail, calendars and financial systems. The same standards apply to business and industry information held by the Commission.

A Security Threat and Risk Assessment must be conducted to:

- Determine if business information systems provide sufficient protection for the information being shared;
- Define controls to manage information sharing;
- Reduce the risk of social engineering; and,
- Identify access control requirements.

### **6.11 - Electronic commerce services**

Information in electronic commerce information systems must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.

#### **a) Electronic commerce**

Prior to initiating or implementing electronic commerce information systems Information Custodians must:

- Ensure that the Security Threat and Risk Assessment is conducted and addresses threats and risks related to electronic commerce;
- Confirm that a Privacy Impact Assessment has been conducted and approved;
- Determine the security classification of the information and information system(s) involved;

- Ensure that the user notification and acceptance of terms and conditions of use complies with Commission policies and standards;
- Ensure multi factor authentication is used commensurate with the sensitivity and value of the information;
- Develop and implement processes to maintain content currency;
- Confirm the information system has received security certification and accreditation; and,
- Develop Disaster Recovery Plans.

**b) On-line transaction security**

To maintain the confidentiality, integrity and availability of on-line transactions in information systems, Information Custodians are responsible for ensuring information systems containing on-line transactions implement security controls commensurate with the value and sensitivity of the information.

Security controls must be implemented to prevent incomplete transmission, misrouting, repudiation of transaction, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials;
- Using digital signatures;
- Using cryptography to protect data and information;
- Establishing secure communications protocols; and,
- Storing on-line transaction details on servers within the appropriate network security zone.

**c) Payment card transaction security**

Information Custodians are responsible for ensuring that information systems used for processing payment card transactions or connected to payment card transaction processing systems comply with the Payment Card Industry Data Security Standard.

The Payment Card Industry Data Security Standard V2.0 has 12 high-level requirements:

- Install and maintain a firewall configuration to protect cardholder data;
- Do not use vendor-supplied defaults for system passwords and other security parameters;
- Protect stored cardholder data;
- Encrypt transmission of cardholder data across open, public networks;
- Use and regularly update anti-virus software or programs;
- Develop and maintain secure systems and applications;
- Restrict access to cardholder data by business need to know;
- Assign unique ID to each person with computer access;
- Restrict physical access to cardholder data;
- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes; and,
- Maintain a policy that addresses information security for all personnel.

Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.

**d) Security of publicly available information**

Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.

Information Owners must approve the publication, modification or removal of information on publicly available information systems. Information Owners are responsible for maintaining the accuracy and integrity of the published information.

Information Custodians are responsible for developing, documenting and implementing Security controls to:

- Maintain the integrity of published information;
- Prevent the inappropriate release of sensitive or personal information;
- Monitor for unauthorized changes; and,
- Prevent unauthorized access to networks and information systems.

## 6.12 - Monitoring

Audit logs recording user activities, exceptions and information security events must be produced and kept to assist in access control monitoring and future investigations.

### a) Audit logging

Information Custodians must ensure that audit logs are used to record user and system activities, exceptions and information security and operational events including information about activity on networks, applications and systems. Information Custodians will determine the degree of detail to be logged based on the value and sensitivity of information assets, the criticality of the system and the resources required to review and analyze the audit logs. Audit logs should include, when relevant, the following information:

- User identifier;
- Dates, times and details of key events (e.g., logon and logoff);
- Logon method, location, terminal identity (if possible), network address;
- Records of successful and unsuccessful system access attempts;
- Records of successful and unsuccessful data access (including record and field access where applicable) and other resource access attempts;
- Changes to system configuration;
- Use of privileges;
- Use of system utilities and applications;
- Files accessed and type of access (e.g., view, read, modify, delete);
- Network addresses and protocols;
- Alarms raised by the access control system; and,
- Activation and de-activation of protection systems (e.g., anti-virus, intrusion detection).

Audit logs may contain confidential data and access must be restricted to personnel with 'need-to-know' privileged access and be protected accordingly.

Information Custodians should not have the ability to modify, erase or de-activate logs of their own activities. There may be cases where IT staff responsibilities overlap to an extent this is not possible.

If audit logs are not activated, this decision must be documented and include the name and position of the approver, date and a rationale for de-activating the log.

### **b) Audit log retention**

Audit logs must be:

- Retained according to the approved retention schedule for the system or information asset; and,
- Retained indefinitely if an investigation has commenced which may require evidence be obtained from the audit logs.

### **c) Response to alarms**

Information Custodians must establish and document alarm response procedures to ensure alarms are responded to immediately and consistently.

Under extreme threat situations, Information Custodians should have documented authority to shut down all or part of a system or network when the alarm indicates severe unacceptable threats are present. When exercising this authority Information Custodians must report the circumstances to management and Information Owners as soon as possible.

Normally, the response to an alarm will include:

- Identification of the alarm event;
- Isolation of the event including affected assets;
- Identification and isolation or neutralization of the source;
- Corrective action;
- Forensic analysis of event;
- Action to prevent recurrence; and,
- Securing of audit logs as evidence.

Some alarms indicating a system or network intrusion will require that the affected system or network not be shut down or removed from the network until a forensic analysis has taken place. This special measure is taken to avoid unintentionally notifying an attacker they have been discovered.

### **d) Monitoring the use of information systems**

The use of information systems must be monitored and the result of the monitoring activities must be regularly reviewed.

Information Custodians must ensure that the use of information systems can be monitored to detect activities including: authorized and unauthorized accesses, system alerts and failures. Information Owners and Information Custodians must identify the activities to be reported. Information custodians must implement, manage and monitor logging systems for:

- Authorized access, including:
  - User identifier,
  - Date and time of log on and log off,
  - Type of event(s),
  - Files accessed, and,
  - Programs, privileges and/or utilities used;
- Privileged operations, including:
  - Use of privileged accounts (e.g., System Administrator, Data Base Administrator)
  - System start-up and shutdown, and,

- Input/Output device attachment and/or detachment;
- Unauthorized access attempts, including:
  - Failed or rejected user actions, data access or other resource attempts,
  - Access policy violations and notifications for network gateways and firewalls, and,
  - Alerts from intrusion detection systems;
- System alerts or failures, including:
  - Console alerts or messages,
  - System log exceptions,
  - Network management alarms, and,
  - Access control system alarms; and,
  - Changes to, or attempts to change, system security settings and controls.

**e) Review of monitoring activities**

Information Custodians must set up and document processes for the review of audit logs based on the Information Owners assessment of the value and sensitivity of the information assets, the criticality of the system and the resources required for review.

Audit log reviews should:

- Prioritize reviews of high value and highly sensitive information assets,
- Be based on a documented security threat and risk assessment,
- Utilize automated tools to identify exceptions (e.g., failed access attempts, unusual activity) and facilitate ongoing analysis and review.
- Monitoring should be tested at least annually to ensure that desired events are detected. Analysis of monitoring activities can indicate:
  - The efficacy of user awareness and training and indicate new training requirements;
  - Vulnerabilities that could be, or that are being, exploited; or
  - Increases or decreases in unauthorized access attempts or unauthorized use of privileges.

**f) Privileged activities logged**

Privileged users typically have extensive system permissions not granted to most users. Information Custodians must ensure that the activities of privileged users are regularly reviewed including logging:

- Event occurrence times;
- Event details, such as files accessed, modified or deleted, errors and corrective action;
- Identity of the account and the privileged user involved; and,
- The system processes involved.

**g) Reporting and logging faults**

Information Custodians must implement processes for monitoring, reporting, logging, analyzing and correcting system faults reported by users and automated detection systems.

Fault logging requirements should be determined through a security threat and risk assessment. Fault management reporting should include:

- Description of fault including date/time, location, extent of fault;
- Analysis of probable source/cause;
- Actions taken to respond to and/or resolve the fault; and,
- Corrective action taken.

#### **h) Synchronization**

Computer clocks shall be synchronized for accurate reporting.

System administrators must synchronize information system clocks to:

- The local default switch gateway, domain controller; or,
- Federal government approved clock host.

## Chapter 7 - Access Control

This chapter identifies the mechanisms that restrict access to Commission information and information assets. Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by legislation that protects particular types of information (e.g., personal, sensitive or industry confidential) and by business requirements.

Access control policies provide the blueprint for the management of user access, authorizations and control mechanisms for computer networks, operating systems, applications and information. This chapter identifies security best practices and responsibilities for administrators and personnel.

### 7.1 - Business requirement for access control

#### a) Access control policy

Access to information systems and services must be consistent with business needs and be based on security requirements. An access control policy for each information system must be created.

Information Custodians are responsible for establishing, documenting and approving access control policies which must:

- Support and enable business requirements;
- Be based upon Security Threat and Risk Assessments; and,
- Include classification of assets.
- Consider both physical and logical access to assets;
- Apply the "need to know" and "least privilege" principles;
- Require access by unique user identifiers or system process identifiers to ensure that all access actions are auditable; and,
- Have permissions assigned to roles rather than individual user identifiers when possible.

The access control policy must be communicated to personnel as part of awareness training.

#### b) Access control policy management

Information Custodians are responsible for establishing processes to manage the access control policies, including:

- Ensuring the process is communicated to all personnel;
- Documenting processes for user registration and deregistration;
- Segregating roles and functions (i.e. access requests, access authorization, access administration);
- Defining rules for controlling access to privileged system functions;
- Identifying roles and/or functions which require multi factor authentication; and,
- Identifying and justifying exceptional cases where there is a need for enhanced personnel security screening for sensitive assets.



### c) Review of access control policy

Information Custodians must conduct periodic reviews of the access control policy as part of an ongoing process for risk management, security, and privacy. Reviews must be conducted:

- Annually at a minimum;
- Prior to the introduction of new or significantly changed systems, applications or other services or major technology changes;
- When the threat environment changes or new vulnerabilities arise; and,
- Following significant Commission staff re-organization as appropriate.

## 7.2 - User access management

There must be a formal user registration and de-registration process for granting access to all information systems to ensure that all access actions are traceable to an identifiable individual or process.

### a) Registration

Information Custodians are responsible for managing access to the assets under their control and must implement registration processes which:

- Requires custodians to approve all access rights. This process should:
  - Ensure access requests are approved by the supervisor/manager of the user requesting access, and,
  - Ensure the reasons for requesting access are consistent with job responsibilities;
- Maintain records of access right approvals;
- Ensures personnel understand the conditions of access and, when appropriate, have signed confidentiality agreements;
- Ensures accesses are traceable to an identifiable individual or process;
- Ensures each user is assigned a single unique identifier for accessing information systems except when:
  - Required to meet limitations of technology; or,
  - Required to meet unique business requirements provided the rationale is documented and approved by the Information Custodian as appropriate.
- Restricts access by using predefined role permissions where possible; and,
- Provides secure and separate transmission of the user identifier and password to the user; and,

### b) Deregistration

Information Custodians must formally assign responsibilities and implement processes to:

- Remove access privileges for employees no longer with the organization by midnight of the employee's last day;
- Promptly review access rights whenever a user changes duties and responsibilities;
- Promptly review access rights whenever the user's branch or department is involved in significant reorganization;
- Review access privileges for employees on extended absence or temporary assignments within 10 working days of the change of status;

- Remove access privileges for employees terminated for cause concurrent with notification to individual; and,
- Quarterly check for and remove inactive or redundant user identifiers.

### **c) Security Screening**

The allocation and use of system privileges must be restricted and controlled to prevent unauthorized access to multi-user information systems.

Information Custodians are responsible for authorizing system privileges and must:

- Identify and document the system privileges associated with each information system or service;
- Ensure the process for requesting and approving access to system privileges includes management or information owner approval(s) prior to granting of system privileges;
- Ensure processes are implemented to remove system privileges from users concurrent with changes in job status (e.g., transfer, promotion, termination);
- Limit access to the fewest number of users needed to operate or maintain the system or service;
- Ensure the access rights granted are limited to and consistent with the users' job function and responsibilities;
- Maintain a record of users granted access to system privileges;
- Ensure use of system privileges is recorded in audit logs;
- Implement processes for ongoing compliance checking of the use of system privileges; and,
- Implement processes for regular review of authorizations in place to confirm that access is still needed and that the least number of users needed have access.

User identifiers with system privileges must only be used for performing privileged functions and not used to perform regular activities. User identifiers established to perform regular activities must not be used to perform privileged functions.

The design of information systems should include processes for performing regular maintenance activities which avoid the requirement of system privileges.

System acquisition and development should encourage use of programs which minimize the need for users to operate with system privileges.

Privileged users should:

- Not read the data of an information asset unless authorized; and,
- Be permitted to view, but not alter, user activity logs as part of security safeguards.

### **d) Managing the issuance of passwords**

The Commission must formally designate individuals who have the authority to issue and reset passwords. The following applies:

- Passwords shall only be issued to users whose identity is confirmed prior to issuance;
- Individuals with the authority to reset passwords must transmit new or reset passwords to the user in a secure manner (e.g., using encryption, using a secondary channel, phone call);
- Whenever technically possible temporary passwords must be unique to each individual and must not be easily guessable;
- Passwords must never be stored in an unprotected form; and,

- Default passwords provided by technology vendors must be changed to a security hardened password compliant during the installation of the technology (hardware or software).

#### **e) Access rights review**

Information Custodians must formally review user access rights at regular intervals. Information Custodians must implement formal processes for the regular review of access rights. Access rights must be reviewed:

- Annually;
- More frequently for high value information assets and privileged users;
- When a user's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect a user's need to access information assets;
- As part of a major reorganization, or the introduction of new technology or applications; and,
- When Information Custodians change the access control policy the access rights must be reviewed.

Review of access rights must include the following:

- Confirmation that access rights are based on the "need to know" and "least privilege" principles;
- Confirmation that all members of the group/role have a need to know;
- Reviews and verification of access control lists are dated and signed by the reviewer and kept for audit purposes; and,
- Confirmation that changes to access rights are logged and auditable.

### **7.3 - User responsibilities**

Users must follow good security practices in the selection and use of passwords.

#### **a) Selection of passwords**

The effectiveness of access control measures is strengthened when users adopt good security practices for selecting passwords. When selecting passwords users must:

- Select complex passwords;
- Avoid using the user name or any proper names of the user;
- Avoid patterns that look complex, but are not; and,
- Avoid using the same password for multiple accounts;

A complex password is defined as being at least 12 characters long and containing at least one numeral (e.g., 1-9,0) or non-alphanumeric keyboard symbols (e.g., ! \$ # %).

For mobile devices connecting to the Commission messaging server, the following password rules apply:

Passwords must contain a minimum of 4 characters if the device is set to wipe after 10 failed login attempts or 6 characters if no wiping is configured;

### **b) Password change**

Passwords must be changed:

- During installation of computer hardware and or software which is delivered with a default password;
- Immediately if a password is compromised or if compromise is suspected. If compromise has taken place or is suspected; and,
- Comply with password change instructions issued by an automated process (e.g., password lifecycle replacement) or an appropriate authority.

A user must not re-use old passwords when selecting a new password.

Privileged accounts have wider and more powerful access rights to information assets. Users authorized to create or who hold privileged accounts must use passwords which are at least 15 characters where technically feasible.

### **c) Protection and use of passwords**

Passwords are highly sensitive and must be protected by not:

- Sharing or disclosing passwords;
- Permitting anyone to view the password as it is being entered;
- Writing down a password;
- Storing other personal identifiers, access codes, tokens or passwords in the same container as the token;
- Keeping a file of passwords on any computer system, including mobile devices unless that file is encrypted with a process approved by the Senior Network Security Analyst;
- Employing any automatic or scripted logon processes for personal identifiers; and,
- Using personal identifiers, access codes, or passwords associated with Commission accounts for non-Commission purposes.
- Divulging your password to anyone. Legitimate IT technical support staff such as systems administrators, helpdesk and security will not ask users for their passwords.

### **d) Protection of unattended equipment**

Users must help prevent unauthorized access to information systems by securing unattended equipment, by:

- Locking or terminating information system sessions before leaving the equipment unattended;
- Enabling a password protection features on the equipment (e.g., screen savers on workstations);
- Shutting down and restarting unattended workstations at the end of each workday;
- Enabling password protection on mobile devices including portable storage devices; and,
- Being aware of their responsibility to report security weaknesses where the above controls have not been applied.

Commission workstations and other devices used for information system access must automatically activate screen savers or equivalent locking systems after 15 minutes of inactivity or less.

**e) Securing the work space**

Users should secure their work space whenever it is not supervised by an authorized person, including during short breaks, attendance at meetings, and at the end of the work day.

- Securing the work space includes:
- Clearing desk tops and work areas;
- Securing documents and portable storage devices in a locked desk or file cabinet;
- Ensure outgoing and incoming mail is appropriately secured;
- Restarting workstations at the end of each work day;
- Locking doors and windows; and,
- Checking fax machines and printers to ensure that no sensitive information is waiting to be picked up.

**f) Secure work habits**

Users must develop and implement security conscious work habits to reduce the likelihood of unauthorized viewing, access or disclosure of sensitive information. Security conscious work habits include:

- Ensuring sensitive information is protected from accidental viewing by persons passing through the work space;
- Ensuring that only the documents required for current work are out of their normal file cabinet;
- Covering up, filing or storing paper documents when visitors are present in the work area;
- Clearing, changing or turning off the computer screen (e.g., minimize open Windows, lock the PC) so that sensitive information is not displayed when visitors are present in the work area; and,
- Not discussing sensitive information in open work spaces or public areas.

## 7.4 - Network access control

Users must only be provided access to the information systems they have been specifically authorized to use.

**a) Access to network services**

Information Custodians must enable network services needed to support business requirements (e.g., by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers.

Information system network access must be restricted to the authorized users and systems, using the principle of least privilege, as defined in the access control policies for the information system.

**b) Management controls and processes**

Information Custodians must document processes for management of network access, including:

- Documentation and review of implemented network access controls;
- Identification of threats, risks and mitigation factors associated with network services;
- Testing of network access controls to verify correct implementation; and,
- Assisting Information Owners to verify the principle of least privilege is used to minimize access, as specified in the access control policy.

### **c) Remote access to Commission networks or services**

Providers of remote network access services for individuals must:

- Perform a Security Threat and Risk Assessment for each remote access service to determine the authentication methods to be implemented. Factors to be considered include classification of network services, information and information systems accessible from the remote access service;
- Require remote users to connect through Commission designated remote access services or security gateways (e.g., Virtual Private Network, Outlook Web Access); and,
- Require user identification and authorization prior to permitting each remote network connection.

## **7.5 - Network security management**

Physical and logical access to diagnostic ports must be securely controlled to prevent unauthorized use of maintenance or diagnostic facilities.

### **a) Protection of diagnostic ports and services**

To prevent bypassing of information system access controls, Information Custodians must implement access control processes for the physical and logical access controls of the ports, services and systems for diagnostic, maintenance and monitoring activities.

Physical and logical access controls to be considered for implementation include: physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems.

Diagnostic ports must be kept inactive until needed, and kept active for the minimum time required.

Diagnostic services like must be kept inactive until needed, and kept active for the minimum time required. (e.g. VMware SSH)

Access to diagnostic ports from remote locations, or by external parties, or service providers must be authorized by agreements, contracts and conditions of use.

### **b) Segregation based on risk and requirements**

Groups of information services, users and information systems must be segregated on networks and/or servers to isolate information systems, users and networks based on risk and business connectivity requirements to control information flow, minimize unauthorized connection attempts and limit the spread of damage in case of compromise.

Information Custodians must segregate services, information systems and users to support business requirements for information system connectivity and access control based on the principles of least privilege, management of risk and segregation of duties.

Information Custodians must establish network perimeters and control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways, application layer 7 firewalls and reverse proxy servers must be implemented at multiple points throughout the network to provide the required level of control.

The techniques and technologies selected for network segregation must be based on Security Threat and Risk Assessment findings. Factors to consider include:

- The information and information system security classification;
- The trustworthiness of the network, based on the amount of uncontrolled malicious traffic present, the level of device identification and authentication in the networks and sensitivity to eavesdropping (e.g., the Internet is a less trusted network than a controlled server network zone);
- Transparency, usability and management costs of network segregation technologies; and,
- The availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

Network zones should be defined and network perimeters established, according to business requirements and risk as identified in the Security Threat and Risk Assessment. For example, network zones for Public access, core network, wireless network, information system operational management and business applications could be defined, separated by network flow control points.

### **c) Logical and physical network connection control**

Information Custodians must restrict the ability of users to physically and logically connect to networks according to the specific access control policy. Techniques may include:

- Physical cabling protection;
- Physical control of network ports in public areas and meeting rooms;
- Segregated networks for unauthenticated devices;
- User and device authentication prior to issuing network addresses;
- Router access control lists;
- Scanning for unauthorized network equipment (e.g., unauthorized wireless access points, modems); and,
- Virtual LANs.

Direct network connections to information systems must only be permitted if required for information system function. For example, database server hardware should be placed in a network security zone to segregate it from direct network connections by user workstations.

### **d) Wireless networks**

Information Custodians must prevent unauthorized connection to wireless networks through use of identification and authentication techniques as determined by a Security Threat and Risk Assessment.

## **7.6 – Operating System Access Control**

### **a) Information displayed before logon**

Information Owners must ensure that Information Custodians configure logon processes to minimize the opportunity for unauthorized access. This includes:

- Not displaying details about backend systems (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with any unnecessary assistance;
- Displaying a general warning notice that the Information System be accessed only by authorized users;

- Validating logon information only on completion of all input data; and,
- Not displaying passwords in clear text as they are entered.

Default web pages or system management interfaces must not display information about the system that could aid an attacker.

#### **b) Unsuccessful logon attempts**

Information Custodians must configure logon processes to:

- Record unsuccessful logon attempts;
- Allow a limited number of unsuccessful logon attempts;
- Limit the maximum and minimum time allowed for the logon procedure. If exceeded, the system should terminate the logon; and,
- Force a time delay or reject further logon attempts if the limited number of consecutive unsuccessful logon attempts is reached.

A best attempt must be made to follow these rules with the exception being that not all systems are compatible with these rules.

#### **c) Password transmission**

Information Owners and Information Custodians must ensure logon processes are configured to prevent transmission of passwords in clear text.

#### **d) Allocation of unique identifier**

Information Custodians must ensure users are issued unique user identifiers for their use. The process for allocating and managing unique identifiers must include:

- A single point of contact to:
  - Manage the assignment and issuance of user identifiers,
  - Ensure that users, except for privileged users, are not issued multiple identifiers for any one information system or platform, and,
  - Record user status (e.g., employee, contractor);
- Identification of those individuals or positions authorized to request new user identifiers;
- Confirmation that the user has been informed of appropriate use policies;
- Linkages with contract management offices and/or contract managers to identify and maintain the status of identifiers issued to contractors; and,
- Conducting annual reviews to confirm the continued requirement for the user identifier.

To segregate roles or functions, privileged users may be issued multiple identifiers for an information system or platform.

#### **e) Shared user identifiers**

In exceptional circumstances, where there is a clear business benefit identified by the Information Custodian, the use of a positional user identifier for a group of users or a specific job can be used, provided:

- Positional user identifiers are not used for privileged users; and,
- The Senior Network Security Analyst approves the positional user identifier.



#### **f) Enforcing quality password rules**

A password management system must be in place for Information Custodians to provide an effective, interactive storage method that ensures quality passwords.

Information Custodians must ensure password management systems:

- Enforce the use of individual user identifiers and passwords;
- Support user selection and change of passwords using the complex password standard defined in 7.3(a);
- Enforce user change of temporary passwords at first logon and after password reset by an Administrator;
- Enforce regular user password changes every 3 months, including advance warning of impending expiry;
- Prevent re-use of passwords for a period of one year;
- Prevent passwords from being viewed on-screen;
- Store password files separately from application system data;
- Ensure password management systems are protected from unauthorized access and manipulation; and,
- Store and transmit passwords in protected (e.g., encrypted) form.

Exceptions are allowed only where system limitations do not allow the enforcement of these rules. Any exceptions must be approved by the Senior Network Security Analyst.

#### **g) Restriction and control of system utility programs**

Use of system utility programs which may be used to override system and application controls must be restricted.

Information Custodians must limit use of system utility programs by limiting the ability to run such programs to privileged users. Beyond IT administrators, system privileges should only be granted to direct administrators of that specific system.

#### **h) Session time-out**

Information Custodians must implement automatic termination or re-authentication of active sessions after a pre-determined period of inactivity. Some systems may also require a connection duration limit (e.g.; VPN sessions).

Commission information systems must have session time-outs managed by operating system access, application or network infrastructure controls.

Application and network sessions must be terminated or require re-authentication after a pre-defined period of inactivity corresponding with the:

- Sensitivity of the system found in the Security Threat and Risk Assessment;
- Classification of the information being handled; and,
- Risks related to the use of the equipment by too many concurrent users.

The actual timeout value will vary between systems. Some guidelines are:

- Maximum timeout of 15 minutes for systems deemed the highest risk or value; and,
- Maximum timeout of 12 hours for low security systems (e.g.; VPN sessions).

## 7.7 - Information and application access controls

Access to information systems functions and information must be restricted in accordance with the corresponding access control policy.

### a) Information access controls

Information Custodians are responsible for ensuring the implementation of the access control policies for their business applications. Every information system must have an access control policy that specifies access permissions for information and system functions. The access control policy must identify the information and system functions accessible by various classes of users.

The application and information section of the access control policy must specify:

- The information to be controlled;
- The system functions to be controlled; and,
- The roles authorized to access the resources/information and what types of access are permitted (e.g., Create, Read, Update/Write, Delete, Execute) based on business need.

### b) System configuration

Information system access controls must be configurable to allow Information Custodians to modify access permissions without making code changes.

System utilities or functions that can bypass user access controls must be specified in the access control policy.

### c) Segregation of information

Information that is publicly accessible (non-confidential) must be segregated from non-public information. The segregation can be physical or use logical methods or controls (e.g.; file folders/shares, databases, tables, ACL's).

Information Custodians must conduct a Security Threat and Risk Assessment to determine the information system classification level. The information system classification level determines which network security zone the information system must reside.

## 7.8 - Mobile computing and teleworking

Appropriate controls must be implemented to mitigate security risks associated with the use of portable storage devices.

### a) Information protection

Information Custodians must ensure that use of portable storage devices is managed and controlled to mitigate the inherent risks of portable storage devices.

The use of portable storage devices such as laptops or other mobile devices to access, store, or process information increases the risk of information compromise. Portable storage devices are typically small, portable, used in uncontrolled public environments and are easily lost, stolen or damaged.

To ensure that sufficient safeguards are implemented to protect information commensurate with its sensitivity a Security Threat and Risk Assessment must be performed prior to permitting subscription or use of mobile computing services.

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.

Providers of mobile computing services must perform annual risk assessments to identify service-specific risks. Policies, standards, practices and guidelines that treat these risks must be developed, documented and maintained.

#### **b) Human factors**

Information Custodians must provide users of mobile computing services with security awareness training, to ensure that users are:

- Aware of the additional risks and responsibilities inherent in mobile computing and when using portable storage devices;
- Aware that data is to be stored on Commission servers and accessed via mobile computing devices;
- Familiar with operation of the protection technologies in use; and,
- Familiar with the reporting procedure for lost or stolen devices.

#### **c) Risk assessment factors**

The Security Threat and Risk Assessment must consider threats to information and information technology assets, such as:

- Physical theft;
- Use of the portable devices to remotely access Commission networks and systems;
- Data interception;
- Credential theft;
- Unauthorized device use;
- Device destruction;
- Information destruction;
- Covert key logging or password harvester programs; and,
- Malicious and mobile code.

Information classification and sensitivity levels must be considered in the risk assessment.

Minimum information protection safeguards for the use of portable storage devices include:

- Encryption of stored data to prevent information loss resulting from the theft of the mobile or remote device;
- Encryption of data transmitted via public network;
- Access control permissions on a portable storage device must be applied to prevent unauthorised access to information by system users, particularly for multi-user mobile systems;
- Regularly maintained data backups of information stored on portable storage devices using Commission backup facilities to protect against information loss;
- To provide information availability portable storage devices must not be used to store the only copy of a Commission record;

- Physical security of the device must be maintained to protect against asset and information loss; and,
- User authentication to the portable storage device and user authentication for remote access from the device must be implemented in accordance with authentication policies.

**d) Teleworking security controls based on risk assessment**

Information Custodians must ensure that Commission information and information technology assets are adequately protected by implementing security controls supported by a Security Threat and Risk Assessment prior to granting permission for employees to enter into a teleworking arrangement.

The Security Threat and Risk Assessment must consider:

- The sensitivity and classification of information that may be accessed or stored at the teleworking location;
- The physical security of information, information technology assets and the teleworking location;
- Unauthorized information access by people at the teleworking location, either inadvertent or deliberate; and,
- Remote access threats if remote access is utilized.
- Security controls that must be considered include:
- Restriction of permitted information types and classifications at the teleworking location;
- Use of secure cabinets, shredders and other physical security equipment;
- Encryption of data stored at the teleworking location;
- Security awareness training for protection of information and information assets, including clear desk policy, information handling rules, physical security issues and remote access training; and,
- Monitoring and review of teleworking equipment for security events and incident response.

**e) Teleworking agreement**

Teleworking arrangements must be formally authorized and documented.

A documented teleworking agreement between the employer and employee must exist that specifies the following user responsibilities, terms and conditions:

- The expectation that the user will actively protect information and information technology assets;
- Restrictions on the information types or classifications permitted at the teleworking location;
- The requirement to protect information from inadvertent or deliberate disclosure to people at the teleworking location by use of secure cabinets, passwords or shredders;
- The authorized teleworking location and contact information;
- Information backup requirements;
- What equipment and software is supplied by the employee and what is supplied by the employer;
- The terms of use for remote access, if applicable;
- The requirement to meet or exceed specified wireless networking security controls, if wireless networking will be used at the teleworking location;
- The requirement to report security events or unusual activity;
- The right of the province to monitor and investigate security events at the teleworking location, including access to employee owned equipment used for teleworking;
- The requirement to establish and maintain security controls as determined in the Security Threat and Risk Assessment;
- Arrangements for technical support; and,

- The start date, end date, expected work hours and provision for termination of the teleworking arrangement.

**f) Ad hoc teleworking policy**

Controls required for ad hoc teleworking are:

- Restriction of the information types and classifications that may be accessed or utilized while teleworking;
- Use of the Commission secure VPN access;
- If required, use of a Commission terminal server;
- Use of SSL Commission websites (e.g.; webmail, ESS);
- Minimum technical security controls required for non-Commission computing equipment, in particular current anti-virus, personal firewall and current software patches; and,
- Subject to applicable law, the right of the Commission to monitor and investigate security events at the teleworking location, including access to employee owned equipment used for teleworking.

## Chapter 8 - Information Systems Development and Maintenance

This chapter establishes requirements for incorporating security measures into the life cycle of an information system. Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files. For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys.

Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks.

Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

### 8.1 - Security requirements for information systems

#### a) Security controls for information systems

Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information Custodians must conduct a Security Threat and Risk Assessment during the requirements phase when developing, implementing major changes to, or acquiring an information system, to:

- Identify the security requirements necessary to protect the information system; and,
- Work with the Information Owners to assign a security classification to the information and information system.

The Information Custodian must ensure that information system development or acquisition activities are done in accordance with documented requirements, standards and procedures which include:

- Testing the information system to verify that it functions as intended;
- Enforcing change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses; and,
- Using common security processes and services (e.g., authentication, access control, financial management).

#### b) Security requirements at implementation

Information Custodians must ensure that sufficient controls are in place to mitigate the risk of information loss, error or misuse from information systems. Prior to implementation, information systems must be assessed to verify the adequacy of, and document the details of, the security controls used, by completing the requirements stated in the system security plan.

### **c) System Security Plan**

A System Security Plan must be documented and maintained for each information system.

The System Security Plan includes:

- A summary of risks identified in the Security Threat and Risk Assessment;
- Roles and responsibilities for information system security management;
- Specific procedures and standards used to mitigate risks and protect the information system;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures.

## **8.2 - Correct processing in applications**

### **a) Input data validation**

Data input to an information system must be validated to ensure that it is correct and appropriate. Information Custodians must ensure the validity and integrity of data input to information systems by:

- Limiting fields to accept specific ranges of data (e.g., defining out of range values or upper and lower data volume limits);
- Checking for invalid characters in data fields;
- Making key fields mandatory;
- Verifying the plausibility of input data using business rules;
- Protecting against common attacks (e.g., buffer overflows); and;
- Using control balances to verify complete input and processing.

### **d) Internal processing**

Internal processing checks must be performed to minimize the risk of processing failures or deliberate acts leading to a loss of integrity. Information Custodians must require that information systems include internal processing checks to:

- Detect unauthorised or incorrect changes to information;
- Prevent information from being accidentally overwritten;
- Prevent internal information from being disclosed via information system responses;
- Protect against common attacks (e.g., buffer overflows);
- Check the integrity, authenticity or any other security feature of data or software downloaded or uploaded between central or remote computers;
- Maintain audit trails; and,
- Provide error and exception reports.

**e) Message integrity**

Message integrity controls must be used for information systems where there is a security requirement to protect the authenticity of the message content. Information Custodians must determine message integrity requirements during the requirements definition phase of system development or acquisition.

Message integrity controls may include:

- Cryptographic signing; or,
- Checksum or hash functions.

**f) Output data validation**

Data output from an information system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Information Custodians must require that processes are documented to validate the data output from an information system by:

- Reconciling control balances to verify that data is processed accurately;
- Verifying the plausibility of output data using business rules;
- Providing sufficient information for a reader or subsequent information system to determine the accuracy, completeness, precision and classification of the information;
- Maintaining audit trails; and,
- Providing error and exception reports.

### 8.3 - Cryptographic controls

The use of cryptographic controls must be based on the risk of unauthorized access and the classification of the information or information system that is to be protected.

**a) Roles and responsibilities**

The IT department is responsible for the provision of cryptographic services, such as those used for user registration services and key management services, by:

- Establishing policy and providing strategic direction on the use of cryptography;
- Setting standards for cryptographic algorithms and key length;
- Defining where cryptography must be used;
- Approving the use of cryptographic services;
- Defining and maintaining standards for cryptographic controls; and,
- Providing technical advice on the use of cryptography.

Information Custodians must document the use of cryptography in the System Security Plan for the information system.



### **b) Acceptable use of cryptography**

The type and quality of cryptographic controls used in information systems must be based on a Security Threat and Risk Assessment, and include consideration of:

- Confidentiality requirements, in accordance with information classification, labelling and handling requirements;
- Integrity requirements (e.g., for financial payments, personal information);
- Authentication requirements (e.g., proof of identity);
- Other security measures (e.g., for proof of origin, receipt, or ownership);
- Legislation, regulations or policies requiring the use of cryptography;
- Restrictions on the export or use of cryptographic products; and,
- Risks relating to the long-term storage of electronic information (e.g., recovery of encrypted data, long-term key maintenance).

### **c) Management of cryptographic keys**

A key management system based on an agreed set of standards, procedures and methods must be used to support the use of cryptographic controls.

The Senior Network Security Analyst is responsible for managing key management standards and processes, including:

- Selection of cryptographic keys with sufficient lengths;
- Distribution, storage and periodic updating of cryptographic keys;
- Revocation of cryptographic keys;
- Recovery of cryptographic keys that are lost, corrupted or have expired;
- Management of cryptographic keys that may have been compromised; and,
- Management of certificate authorities.

## **8.4 – Security of system files**

The implementation of software on operational information systems providing services must be controlled.

### **a) Changes to operational information systems**

Information Custodians must implement procedures to control software installation on operational information systems providing services to ensure that:

- Updates of operational information systems are planned, approved, impacts assessed, tested, logged and have a rollback plan;
- Operations personnel and end users have been notified of the changes, potential impacts and if required have received additional training;
- New releases of software are reviewed to determine if the release will introduce new security vulnerabilities;
- Modifications to operational software are logged;

- The number of personnel able to perform the updates is restricted and kept to a minimum;
- Development code or compilers are not present on operational information systems; and,
- Vendor supplied software is maintained at the supported level.

#### **b) Pre-Implementation guidelines**

Before an updated or new information system is implemented into the operational environment, checks should be performed to ensure that:

- A Security Threat and Risk Assessment has been carried out;
- Security hardening testing (e.g.; penetration testing, Nessus scanning);
- A Privacy Impact Assessment has been performed;
- Limitations of security controls are documented;
- Performance and capacity requirements can be met and have the capacity to maintain the information system;
- Development problems have been resolved successfully;
- The effects on existing operational information systems are known; and ,
- Arrangements for fall-back have been established if the updated or new information system fails to function as intended.

Steps to perform before the updated or new information system is implemented into the operational environment include:

- Communicate changes to users who may be affected by the change;
- Error recovery and restart procedures should be established;
- Disaster Recovery plans should be developed or updated;
- Operating procedures should be tested;
- Users should be educated to use the information system correctly and securely; and,
- Computer operator's/system administrators should be trained in how to run the information system correctly and securely.

#### **c) Implementation guidelines**

The installation process should include:

- Validating the load or conversion of data files;
- Installing executable code only, and not source code;
- Providing ongoing technical support;
- Implementing new or revised procedures/documentation;
- Discontinuing old software, procedures and documentation;
- Arranging for fall-back in the event of failure;
- Informing the individuals involved of their roles and responsibilities;
- Transferring responsibility for the information system from development teams to operational teams to ensure segregation of duties; and,
- Recording installation activity and documenting in the DRP.

#### **d) Post-implementation guidelines**

Post-implementation reviews should include:

- Security hardening re-testing (e.g.; penetration testing, Nessus scanning);
- Lessons learned and scope for improvements of security controls; and,
- Security incidents and mitigation.

#### **e) Protection of program source libraries**

Access control must be maintained for program source libraries. Information Custodians must implement procedures to control access to program source code for information systems that include:

- Program source code is isolated and stored separately from operational information systems;
- Program source code is contained in protected code repository;
- Privileged users access is defined and monitored;
- A change control process is implemented to manage updating of program source libraries and associated items; and,
- Accesses and changes to program source libraries are logged.

### **8.5 - Security in development and support processes**

Changes to software must be controlled by the use of formal change control procedures.

#### **a) Changes to software during information systems development**

Information Custodians must implement a change control process during development which includes:

- Requiring that change requests originate from authorized personnel;
- Requiring that proposed changes are reviewed and assessed for impact; and,
- Logging all requests for change.

#### **b) Changes to software for operational information systems**

Information Custodians must implement a change control process during the maintenance phase including:

- Requiring that change requests originate from authorized personnel;
- Performing an impact assessment considering items such as the System Security Plan and proposed modifications;
- Documenting fallback plans;
- Documenting approval of changes proposed prior to the commencement of the work;
- Documenting the acceptance tests and approval of the results of acceptance testing;
- Updating the System Security Plan and other system, operations and user documentation with the details of changes in accordance with records management policy;
- Maintaining version control for all changes to the software; and,
- Logging all requests for change.

### **c) Changes to the operating system**

Information systems must be reviewed and tested when operating system changes occur.

Information Custodians must account for:

- Sufficient time for the review and testing of information systems prior to implementation;
- Review of System Security Plans to ensure information systems will not be compromised by the change;
- Information system testing with the changes to the operating system in a separate (i.e. test, stage) environment if and environment exists;
- A roll back plan in the event of change failure; and,
- Update of disaster recovery plans if required.

### **d) Changes to commercial-off-the-shelf software**

Other than vendor supplied patches, commercial-off-the-shelf software must not be modified except in exceptional circumstances when needed for a critical business requirement. This requirement must be documented and approved by the Information Custodian.

A software update management process must be maintained for commercial-off-the-shelf software to ensure the most up-to-date approved patches have been applied and the version of software is vendor supported.

### **e) Preventing information leakage**

Controls must be applied to limit opportunities for information leakage. Information Custodians must implement processes to reduce the opportunity for information leakage in information systems by:

- Scanning for malicious code;
- Monitoring resource usage in information systems;
- Monitoring for unusual access in information systems;
- Identifying and limiting the trusted connections in and out of the Commission network;
- Controlling third party network connections (e.g., only authorized traffic permitted);
- Using software that is considered to be of high integrity; and,
- Regular monitoring of information systems.

### **f) Outsourced information system development**

Controls must be applied to secure outsourced information system development. Information Custodians must consider the following when outsourcing information system development:

- Procurement policy for licensing, ownership and intellectual property rights;
- Escrow arrangements in the event of the failure of the external party;
- Testing of the information system for common vulnerabilities and malicious code;
- Rights of access for audit and certification of the quality and accuracy of the work; and,
- Contractual requirements for quality and security functionality of the information system.

## 8.6 - Vulnerability management

Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks.

### a) Vulnerability response processes

Vulnerabilities which impact Commission information systems must be addressed in a timely manner to mitigate or minimize the impact on operations. Information Custodians must establish processes to identify, assess and respond to vulnerabilities that may impact information systems by:

- Monitoring external sources of information on published vulnerabilities;
- Weekly automated scanning of systems with a vulnerability assessment tool (e.g.; Nessus scanner);
- Assessing the risk of published vulnerabilities;
- Testing and evaluating options to mitigate or minimize the impact of vulnerabilities;
- Applying corrective measures to address the vulnerabilities; and,
- Reporting to the any found vulnerabilities.

The Senior Network Security Analyst must:

- Evaluate vulnerabilities and provide advice on appropriate responses;
- Monitor progress in responding to vulnerabilities;
- Publish summary reports on vulnerability response activities; and,
- When required, initiate incident response processes to address vulnerabilities.

## Chapter 9 - Information Security Incident Management

This chapter establishes requirements for reporting a possible breach of information security as quickly as possible. This includes establishing procedures and processes so that personnel understand their roles in reporting and mitigating security events.

Information security incident management policies identify mechanisms to detect and report when information security events occur and the directives for the consistent management of such events. The information collected about the events can be analyzed to identify trends and to direct efforts continually improve and strengthen the information security infrastructure of the Commission.

### 9.1 - Reporting information security events and weaknesses

#### a) Reporting information security events

Commission personnel and contractors must immediately report all suspected or actual information security events to the IT Department as required by the Information Incident Management Process. Requirements for reporting events must be included in contracts and service agreements.

Information security education for Commission personnel should build trust with users and stress that "to err is human". Positive reinforcement of good reporting practices will help users understand their responsibilities. Users who commit errors that lead to security incidents should receive appropriate training to help prevent future incidents

#### b) Reporting security weaknesses

Commission personnel and contractors using information systems must note and report any observed or suspected security weaknesses in those systems to help assist in maintaining the security of the systems.

Information Custodians must follow the Information Incident Management Process for responding to suspected or actual security weaknesses which includes:

- Ensuring all reports are investigated and handled in a secure, confidential manner; and,
- Ensuring the individual who reported the weakness is advised of the outcome when the investigation is complete.

### 9.2 - Management of information security incidents and improvements

#### a) Information security incident management and response

The IT Department must follow the Information Incident Management Process for reporting, managing, responding to and recovering from information security incidents. The process must include:

- A reporting process that includes the Senior Network Security Analyst;
- When exercising incident management authority, authorized staff must notify senior management of the incident and mitigation activities at the earliest possible time;
- Staff with incident management responsibilities must be appropriately trained and qualified, and their authorization for access to live systems and data delineated formally;
- Processes are established for handling different types of information security incidents, including immediate action for containment, response escalation and contingency plans; and,

- Incident response processes must be documented, tested and rehearsed regularly to evaluate their effectiveness.

#### **b) Information security incident investigation**

Information security incident investigation should be formalized and practiced in accordance with standard investigation techniques:

- Information security incident investigation processes include:
  - Identification of the incident's cause,
  - Planning of corrective action,
  - Implementation of corrective action to prevent recurrence, and,
  - Post-mortem - Reporting action taken;
- Staff with responsibilities for information security investigations (Senior Network Security Analyst) must be aware of processes for securing potential evidence such as technology assets (e.g., PCs), audit logs, audit trails, voice mail and e-mail accounts for analysis and as potential evidence in legal proceedings;
- Inappropriate use of information and technology resources requires that within 48 hours the investigating officer contact:
  - In the case of an employee the individual's excluded Manager, and,
  - In the case of a contractor or business partner the contract manager.
- When criminal activity is suspected, the investigating officer must ensure that the appropriate law enforcement authorities are contacted. However, before contacting law enforcement authorities the Risk Management Branch and Government Security Office and the Office of the Government Chief Information Officer must be consulted;
- On resolution of an information security incident or weakness, the investigating officer must prepare a report that includes a detailed problem analysis, action(s) taken, and recommendations for corrective action or improvements; and,
- Information security incident reports must be submitted to Information Owners, Information Custodians and senior management as part of security program management.

#### **c) Learning from past incidents**

Continuous improvement of security incident management processes includes:

- Monitoring incidents using statistical analysis of frequency, types and locations of security incidents;
- Analysis of incidents, responses and successful containment;
- Determining requirements for user awareness and training;
- Improving the security of information systems through monitoring and reporting;
- Integrating automated alarms and other security incident detection technology with user reporting, checking logs and auditing systems; and
- The consolidating of reporting for all security weaknesses, threats, events and incidents to avoid duplication and establish a consistent approach.

Personnel who regularly ignore policy should be subject to a disciplinary process that includes notification of their manager and suspension of privileges for repeated offences.

#### **d) Monitoring for security breaches**

The Senior Network Security Analyst is responsible for monitoring for and evaluating information security incidents by:

- Using statistical analysis of incident frequency, type and location to identify trends;
- Ensuring incident reports and trends are used to promote continuous improvement of security policies and processes, security awareness and training programs, and business continuity and disaster recovery plans;
- Advising Information Owners and Information Custodians of evolving security exposures and mitigation strategies;
- Evaluating the effectiveness of incident management, response and reporting; and,
- Evaluating the effectiveness of information security technologies.

Potential types of security incidents to be reported include:

- Breaches of privacy and/or confidentiality;
- Denial of service;
- Detection of network probing;
- Detection of malicious code (e.g., virus, worm, Trojan Horse);
- Errors due to incomplete or inaccurate data;
- Outgoing network traffic not associated with typical business processing;
- Repeated attempts of unauthorized access;
- Repeated attempts to e-mail unknown internal accounts;
- System activity not related to typical business processing; and,
- System failures and loss of service.

#### **e) Collection of evidence**

Investigations into information security incidents must ensure evidence is collected, retained and presented. At the outset of an information security investigation it may not be known if legal or disciplinary actions will result. Evidence must only be collected by individuals authorized by the Commission senior management.

Evidence collection procedures must be documented by the Senior Network Security Analyst.

Investigative processes must follow the rules of evidence to ensure relevance, admissibility and materiality.

Information Owners and Information Custodians in receipt of a legal order to produce electronic evidence must immediately contact the Senior Network Security Analyst.



## Chapter 10 - Disaster Recovery & Business Continuity Management

This chapter provides direction from a security focus for planning the resumption of business or services where a major disruption has occurred. The Commission is required to be prepared and to re-establish business or services as swiftly and smoothly as possible. Development and review of these plans include the evaluation of security risks.

### 10.1 - Information security aspects of Disaster Recovery and Business Continuity management

#### a) Disaster Recovery

When developing new documentation to be part of the DRP, each new document must be reviewed for security considerations. There are several sections of the DRP that are reviewed/revised yearly by IT Security staff including (but not limited to) firewall, third party gateway, VPN, etc.

#### b) Business continuity

During each year's annual review of the BCP if there are major changes to the core of the document it must be evaluated by IT Security staff. The purpose of the review is to determine if there are risks associated with implementing the BCP and create a mitigation plan.

## Chapter 11 - Compliance

The chapter describes requirements for verifying that information systems comply with relevant statutory, regulatory, and information security contractual clauses. Compliance policies identify what to do to ensure that the Commission is in compliance with applicable laws and policies. Processes to monitor the extent in which information systems follow policies include conducting security reviews, assessments and the systematic analysis of logged information.

### 11.1 - Compliance with legal requirements

The statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained.

#### a) Legal requirements

Information Custodians are responsible for ensuring that statutory, regulatory, policy and contractual requirements of each information system are:

- Identified and documented when commencing a system development or enhancement initiative;
- Reviewed prior to, or concurrent with, changes to legislation, regulation or policy; and,
- Explicitly identified in contracts and service agreements, and included in:
  - Privacy Impact Assessments,
  - Security Threat and Risk Assessments,
  - System Security Plans,
  - Risk Management Plans, and,
  - Business Continuity Plans.

Controls must be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licensing.

#### b) Intellectual property rights of external creators and owners

Controls must be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licensing.

Information Owners and Information Custodians must protect intellectual property by:

- Ensuring that information and software is only acquired from reputable vendors;
- Maintaining proof or evidence of ownership or right to use;
- Adhering to the terms and conditions of use associated with intellectual property;
- Ensuring the maximum number of users permitted is not exceeded;
- Implementing processes to detect unlicensed information (e.g., ISO standards documents) and software or expired licenses;
- Requiring the removal of unlicensed information and software from Commission information systems;
- Informing personnel of Commission policies including those pertaining to appropriate use of Commission resources;
- Ensuring licensed intellectual property is securely removed from electronic media prior to media disposition; and,
- Complying with terms and conditions for information and software obtained from public networks (e.g., "free for personal use only", open source).

### **c) Records management**

To ensure the Information Security Policy and supporting processes enable compliance with legal and policy requirements for government records, Commission records must be protected from loss, destruction and falsification.

The Document Disposal Act defines requirements for the disposal of government records.

Policy requirements for records management are in Core Policy and Procedures Manual 12.3.3 - Information Management, and the Commission's internal Records Management Policy

### **d) Data and personal information protection**

The Freedom of Information and Protection of Privacy Act requires personal information to be protected using 'reasonable security measures'.

Policy requirements for protecting data and personal information are found in Core Policy and Procedures Manual 12.3.3 - Information Management and the Freedom of Information and Protection of Privacy Act Policy and Procedures Manual.

This Information Security Policy includes detailed controls which enable and support the protection of Commission information and information systems.

### **e) Deterring unauthorized and inappropriate use of information systems**

Controls must be in place to deter misuse of information systems. Information Custodians must monitor information system usage to prevent, detect and respond to unauthorized or inappropriate use by:

- Ensuring audit logs contain sufficient detail to detect and trace inappropriate usage;
- Implementing processes to analyze audit logs to identify potential misuse of information systems;
- Implementing system rules to prevent access to undesirable Internet sites;
- Implementing content inspection and filtering tools (e.g., for e-mail and web traffic);
- Immediately notifying personnel of detected misuse (e.g., Websense for Internet blocking);
- Ensuring that security incidents are investigated in accordance with policy; and,
- Determining, in consultation with management, if disciplinary action, including dismissal, cancellation of contract and/or other legal remedies are warranted for personnel who have made unauthorized or inappropriate use of information system resources.

Prior to implementing information system monitoring processes Information Custodians must ensure:

- Monitoring activities will be compliant with legal, policy and contractual requirements and obligations;
- Personnel are informed that specific activities may be monitored; and,
- Access to data gathered through monitoring processes is restricted on a 'need to know' and 'least privilege' basis to the fewest possible number of users.

#### **f) Regulation of cryptographic controls**

Cryptographic controls must be used in conjunction with relevant agreements, laws and regulations. When cryptographic controls are used, Information Custodians must:

- Ensure that the use of cryptographic control(s) is supported by an Information Security Threat and Risk Assessment;
- Consult with the Senior Network Security Analyst regarding the records management, electronic commerce, information access, privacy and security issues prior to acquiring cryptographic controls;
- Ensure encrypted Commission information assets do not become unavailable due to unavailability or loss of cryptographic keys by implementing a process to manage cryptographic keys; and,
- When acquiring cryptographic controls from outside Canada, the procurement must be from a reputable vendor who can provide reasonable assurance on the legality of import into Canada.

The Senior Network Security Analyst will:

- Develop and document cryptographic key management processes;
- Provide guidance and assistance to Information Custodians in the selection and use of cryptographic controls; and,
- Establish and publish cryptographic standards.

## **11.2 – Compliance with security policies and standards**

### **a) Compliance roles**

Management must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards.

Information Custodians must ensure security policies and processes are implemented and adhered to by:

- Conducting periodic self-assessments;
- Ensuring personnel receive regular information security awareness updates; and,
- Initiating independent assessments, reviews or audits to assess compliance to policy.

When review processes indicate non-compliance with policies, Information Custodians must:

- Determine cause(s);
- Assess the threats and risks of non-compliant processes; and,
- Develop plans to implement corrective action.

### **b) Review of controls**

The Commission must develop an annual plan which identifies information systems scheduled for a security review in each fiscal year. Mission critical information systems are to be reviewed at least annually.

**c) Review of implementation of information incident report recommendations**

Information Owners and Information Custodians must ensure that recommendations from information incident reports are addressed.

The Senior Network Security Analyst may perform compliance reviews or audit of the implementation of recommendations from information incident reports, when necessary. Information Custodians must support the audit activities.

**d) Technical compliance checking**

Information Custodians or the Senior Network Security Analyst must regularly test information system technical control compliance by using automated tools to:

- Detect network intrusion;
- Conduct penetration testing;
- Determine if information system patches have been applied;
- Confirm that system technical controls have been implemented and are functioning as designed; and,
- Perform technical compliance checking as part of the system change management process to verify that unauthorized connections and/or systems changes have not been made.

Personnel responsible for technical compliance checking must ensure that:

- Affected Information Custodians, Information Owners and operations personnel are consulted prior to initiating tests; and,
- The Information Custodians responsible for monitoring are notified prior to testing to prevent triggering false security alarms from the infrastructure.

**e) Reporting results**

Managers responsible for technical compliance checking and Information Custodians must:

- Assess results of testing and promptly develop action plans to investigate and mitigate identified exposures in consultation with the Senior Network Security Analyst;
- Provide Information Owners and the Senior Network Security Analyst copies of test results and action plans;
- Provide the Senior Network Security Analyst with the internal or external audit reports immediately upon receipt; and,
- Maintain records, in accordance with established records schedules, of tests for subsequent review by internal and external auditors.

### 11.3 Information systems audit considerations

Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.

#### a) Management of information systems compliance checking

Prior to commencing compliance checking activities such as audits, risk and controls reviews, monitoring or security reviews of operational information systems, the Manager responsible for the compliance checking activity, Information Custodians must define, document and approve the activities by:

- Determining the scope, duration and level of detail of the compliance checking activity;
- Limiting access rights to operational information systems for compliance checking personnel to "read only";
- Determining handling requirements for copies of files made by compliance checking personnel including:
  - Establishing a separate environment for the analysis of files,
  - Restricting access to those files,
  - Logging the accesses made to those files, and,
  - Erasing files at the conclusion of compliance checking activities unless needed to support report findings;
- Identifying special testing or processing which may impact the operational information system (e.g., penetration tests, server vulnerability assessments) and by:
  - Notifying the Senior Network Security Analyst prior to compliance checking activities to prevent triggering false security alarms from the infrastructure, and,
  - Scheduling tests to minimize disruption;
- Submitting the reports of penetration tests or vulnerability assessments to the Senior Network Security Analyst immediately upon receipt.

#### b) Protection of information system audit tools

Access to system audit tools must be controlled to prevent misuse or compromise. Managers responsible for compliance checking activities and Information Custodians must control the use of audit tools by:

- Restricting access to authorized personnel who have a need-to-know;
- Installing or enabling specialized audit tools for the duration required by the compliance checking activity;
- Removing information system access at the conclusion of the compliance checking activities; and,
- Notifying the Senior Network Security Analyst prior to the use of audit tools.

## Glossary

**Accreditation** - the final approval to authorize operation of an information system and to explicitly accept the risk to Commission operations (including mission, functions, image, or reputation), assets, or individuals, based on the implementation of an agreed upon set of security controls.

**Ad hoc telework** - occasional telework that may not have a formal agreement in place. (See: telework)

**Application** (business application) - a collection of computer hardware, computer programs, databases, procedures and knowledge workers that work together to perform a related group of services or business processes.

**Assets** - for the purposes of information security policy, information in all forms and media, networks, hardware, software and application systems.

**Audit** - is an examination of the facts to render an opinion and would include testing evidence to support the opinion.

**Audit logs** - includes all types of event logs including (but not limited to) security, audit, application, access and network across all operating system platforms.

**Authentication** - the verification of the identity of a person or process.

**Availability** - information or information systems being accessible and usable on demand to support business functions.

**Business Continuity Plan (BCP)** - the procedures and information necessary for the timely recovery of essential services, programs and operations, within a predefined timeframe. The BCP includes the recovery following an emergency or a disaster that interrupts an operation or affects service or program delivery.

**Business information systems** - internal administrative and productivity information systems that support the organization such as e-mail, calendars and financial systems.

**Capacity management** - the process of determining the system capacity needed to deliver specific performance levels through quantification and analysis of current and projected workload.

**Certification** - See: security certification

**Commercial-off-the-shelf (COTS)** - commercially available products that can be purchased and integrated with little or no customization.

**Compliance checking** - in the context of the Information Security Policy, includes: an audit; risk and controls review; security review; and monitoring of an information system.

**Confidentiality** - information is not made available or disclosed to unauthorized individuals, entities or processes.

**Control** - (of a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure. Where the information in a record directly relates to more than one public body, more than one public body may have control of the record.

**Control balances** - computational aids for data verification e.g., records counts, row and column counts, subtotals, etc.

**Cryptographic Keys** - a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of data into encrypted data and the transformation of encrypted data into data during decryption. The cryptographic algorithm ensures that only someone with knowledge of the key can reproduce or reverse the transformation of data.

**Cryptography** - the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, or prevent its unauthorized use.

**Custody** - (of a record) means having physical possession of a record, even though the public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing and providing security.

**Data** - See: Information.

**Diagnostic Ports** - ports, services and systems used for diagnostic, maintenance and monitoring activities for managing information system performance, function or capacity. Examples include: physical network switch diagnostic ports, logical management services such as SNMP and modems for remote maintenance.

**Digital signing** - refers to an attempt to mimic the offline act of a person applying their signature to a paper document. Involves applying a mathematical algorithm, usually stored on and as part of the users' private key, to the contents of a body of text. This results in an encrypted version of the document (this is referred to as the 'digitally signed' document) that can only be decrypted by applying the user's public key. (Also digitally signing, digital signature)

**Disaster Recovery Plan (DRP)** - the procedures and information necessary to recover critical IT functions from any event that may interrupt an operation or affect service or program delivery, within the timeframes determined in the Business Impact Assessment. The DRP is part of a Commission's overall business continuity plan (Business Continuity Plan or BCP).

**Disposition** - the actions taken regarding information that is no longer needed to support on-going administrative and operational activities in accordance with an approved Records Management Schedule. Directions may include destroy, transfer to the government archives, transfer to inactive records storage space, or retain permanently in unit.

**Electronic agent** - a computer program, or other electronic means, used to initiate an activity or to respond to electronic information, records or activities in whole or in part without review by an individual at the time of the response or activity.

**Electronic commerce** - the exchange of information between government and internal and external stakeholders independently of either participant's computer system. E.g., electronically accessing forms, obtaining payments, sending invoices, receiving tax returns, placing orders and receiving transaction acknowledgements.

**Electronic messages** - includes all forms of electronic messaging such as e-mail, voice mail, instant messaging etc.

**Employee** - is a person employed by the Commission.



**Essential services** - Essential business processes are those processes defined as mission-critical and business- priority and essential to delivery of outputs and achievement of business objectives. Business activities and resources are the essential elements that combine to make up each essential business process.

**Event** - is an identified occurrence of a system or service state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

**External Party** - a person external to the Commission.

**Fault** - an error or failure in either software or hardware.

**Firmware** - programming that is inserted into programmable read-only memory becoming a permanent part of a computing device.

**Hardware** - includes (but not limited to) servers, desktop computers, printers, scanners, fax machines, photocopiers, multi-function devices, routers, communications and mobile equipment, cell phones, mobile devices, removable media.

**Information** - the data in context. The meaning given to data or the interpretation of data, based on its context, for purposes of decision making.

**Information asset** - includes all data, information and intellectual property.

**Information classification label** - a designation indicating the information classification, e.g., "Public", "Confidential", "Internal Only".

**Information Custodians** - maintain or administer information resources on behalf of the Information Owner. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource. Information Custodians are staff in the Commission IT or IS Department.

**Information labelling** - affixing a physical or electronic label identifying the security category of a document, file or records series in order to alert those who handle it that it requires protection at the applicable level.

**Information Owners** – the person with the primary responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.

**Information processing facilities** - the physical location housing any information processing system, service or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal.

**Information Security** - preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

**Information security activities** - management and technology programs to protect government information assets.

**Information security architecture** - a strategy that consists of layers of policy, standards and procedures and the way they are linked to create an environment in which security controls can be easily established.

**Information Security Classification** - a system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability. (also classification, information classification, security classification)

**Information Security Event** - See: event.

**Information Security Incident** - is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (ISO/IEC TR 18044:2004) Information security incidents may include but are not limited to:

- Inappropriate use of government resources causing a service disruption;
- Breaches of privacy and/or confidentiality;
- Denial of service;
- Detection of network probing;
- Detection of malicious code, e.g., virus, worm or Trojan horse;
- Errors due to incomplete or inaccurate data;
- Outgoing network traffic not associated with typical business processing;
- Repeated attempts of unauthorized access;
- Repeated attempts to e-mail unknown internal accounts;
- System activity not related to typical business processing;
- System failures and loss of service.

**Information System** - any equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

**Information System Security Classification** - a system of designating security categories for information systems based on the information security categories of information processed by the information system.

**Information technology asset** - includes owned and leased technology hardware (i.e. physical items), owned or licensed software and related or supporting services.

**Information technology resources** - information and communications technologies, including data, information systems, network services (e.g., Web services; messaging services); computers (e.g., hardware, software); telecommunications networks and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants).

**Information type** - information classes or groupings based on function, usage, attributes or other commonality. E.g., personnel records, invoices, or system documentation are information types. Address, name, or birth date are examples of discrete data elements.

**Integrity** - the characteristic of information being accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated, or unintentional modification.

**Intellectual property** - intellectual property refers to the category of intangible (non-physical) property consisting primarily of rights related to copyrighted materials, trademark, patent and industrial design.

Intellectual property rights are associated with a wide range of products of the human intellect, such as training manuals, publications, map products, videos and computer software. It is important to keep clear the distinction between the items that give rise to intellectual property, such as the manuals and software, and the intellectual property itself, which is the set of rights arising from the creation and development of the items. Simply put, the items are the copies of a particular book, whereas the intellectual property is the copyright in that book.

**Key Management** - the processes for the generation, exchange, storage, safeguarding, use, vetting and replacement of cryptographic keys.

**Least Privilege** - a security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

**Malicious code** - malicious code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources. Types of malicious code can include viruses, worms, Trojans, spyware and denial of service attacks.

**Media** - Material that information is written to and stored on. See: Records.

**Message integrity** - the assurance of unaltered transmission and receipt of a message from the sender to the intended recipient to maintain the completeness, accuracy and validity of the information contained in the message.

**Mission Critical** - processes that, should they not be performed, could lead to loss of life ("safety"), personal hardship to citizens, major damage to the environment, or significant loss in revenue and/or assets.

**Mobile code** - multiplatform computer code that can be downloaded or transmitted across a network that runs automatically on a computer with little or no user interaction.

**Mobile code technology** - software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, VBScript, ActiveX).

**Mobile computing service** - a service that provides access to government systems from Mobile Computing Devices. Distinct from Remote Access Services in that the mobile computing service provides product-specific access to limited applications rather than full standard network access (e.g., Exchange ActiveSync Service).

**Mobile devices** - portable self-contained electronic devices, including portable computers (e.g., laptops), personal digital assistants (PDAs), cell phones, digital cameras, etc.

**Monitoring** - a regular/ongoing check on aspects of operations to identify and correct deviations from policies and standards.

**Multi factor authentication** - this is combining two or more authentication techniques together to form a stronger or more reliable level of authentication. This usually involves combining two or more of the following types: Secret - something the person knows Token - something the person has Biometric - something the person is.

**Need to know principle** - a privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office. The need- to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain records, listing individuals who may access certain records, or installing access controls on automated information systems. The need-to-know principle is especially important in protecting the privacy of individuals as required by the Freedom of Information and Protection of Privacy Act.

**Network Address Spoofing** - forging or faking source network addresses with the intent to obscure, hide or impersonate the actual source device.

**Network infrastructure** - the equipment, information systems and cabling systems used to establish a communication network between Information Systems. Includes routers, switches, hubs, firewalls, transmitters, fibre optic cable and copper cable.

**Network management information** - the information used to manage network infrastructure, including traffic statistics, counters and logs.

**Network pathways and routes** - the physical and logical pathways that comprise the connections within the network infrastructure.

**Network security boundary** - the logical or physical boundary between networks of differing security protection requirements. Network access control devices demark the network security boundaries.

**Network security zone** - a logical entity containing one or more types of services and entities of similar security requirements and risk levels.

**Network segregation** - the separation of groups of users, information systems and services with similar business functions by control of network traffic flow, e.g., by use of security gateways, physically separate networks or access controls.

**Network service agreement** - The contract or agreement between a service provider and a service consumer which defines the services to be delivered and the terms and conditions of delivery.

**Network service provider** - a provider of network services to the Commission which may be internal or external to government.

**Non-repudiation** - the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

**Non-retrievable** - unable to recover the data from any media in any form.

**Outside authorities** - include law enforcement, fire departments, other emergency response authorities, utilities and telecommunications providers.

**Password management system** -An automated process which enforces password rules.

**Personnel** - includes employees and other individuals (e.g., contractors, consultants, volunteers, third-party organizations).

**Portable storage devices** - electronic media including but not limited to laptop and notebook computers, removable hard drives, USB mass storage devices (flash drives, jump drives, memory sticks, memory cards, thumb drives, MP3 players, iPODs and PDAs), zip drives, CDs, DVDs, tapes and diskettes.

**Positional user identifier (userid)** - is a unique system userid assigned to a persistent function or job in circumstances where the personnel filling the job are transitional. Positional userids are issued to a Manager or supervisor who is accountable for the day to day management and assignment of the userid to individuals. E.g., a positional userid could be used if a receptionist position was temporarily filled by short term staff from an employment agency. In these limited circumstances use of positional userids can avoid creating new userids for short term staff.

**Privacy** - the right of an individual to be secure from unauthorized disclosure of information about oneself that is contained in documents.

**Privacy Impact Assessment** - an assessment that is conducted to determine if a new enactment, system, project or program meets the requirement of Part 3 of the Freedom of Information and Protection of Privacy Act.

**Privileged operations** - permissions which allow the user to alter access rights and structures of information systems and/or services.

**Privileged users** - users with permissions to alter access rights and structures of information systems. This includes (but is not limited to) system administrators, network administrators, database administrators, security administrators, web site administrators, system operators and network operators.

**Privileges** - See: privileged operations.

**Reception Zone** - an area where the initial contact between the public and the Commission occurs, where services are provided, information exchanged and access to restricted zones is controlled.

**Record** - includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise.

**Remote access** - the act of using a remote access service to connect to the Commission network or government systems.

**Remote access service** - a service that provides network access to the Commission network or Commission systems from a remote location, e.g., the VPN service.

**Requirements phase** - one component of the System Development Life Cycle. Functional user requirements are formally defined and delineate the requirements in terms of data, system performance, security and maintainability requirements for the system. All requirements are defined to a level of detail sufficient for systems design to proceed. All requirements need to be measurable, testable and related to the business need or opportunity.

**Restricted Access Operations Zone** - a controlled area where access is limited to persons who work there and to escorted visitors. It is usually a standard working area and offices.

**Restricted Access Security Zone** - a strictly controlled area where access is limited to authorized persons and to properly escorted visitors.

**Risk** - Potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.

**Risk and controls review** - an independent and objective assessment of an information system to determine whether the business/system framework has adequate controls to mitigate business, financial, security and general privacy risks.

**Screening** - to verify facts about individuals related to their identity, professional credentials, previous employment, education and skills.

**Secured Path** - a network path that has been protected from eavesdropping, intrusion and data tampering.

**Security categories** - inform employees how to handle records in order to protect them and determine requirements for marking, storage, transport, transmittal and destruction.

**Security certification** - a comprehensive assessment of the management, operational and technical security controls in an information system, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

**Security infrastructure** - the complete set of information security-related systems, policies, standards, guidelines, procedures, resources and physical implementations of information security administration.

**Security Management Systems** - systems that collect, store and manage configuration and operational information about network devices. Includes configuration management databases and log management systems.

**Security posture** - the security status of the technical infrastructure and information systems to known vulnerabilities and attacks.

**Security review** - an independent review with the scope focused on the security framework over the business processes, application and operating environment. Reviews are distinguishable from audits in that the scope of a review is less than that of an audit and therefore the level of assurance provided is lower.

**Security Threat and Risk Assessment** - a component of a risk analysis specifically aimed at identifying security exposures.

**Security weakness** - a weakness in an application, procedure or process that may result in a security incident.

**Security zone** - See: reception zone, restricted access operations zone, restricted access security zone.

**Software** - includes (but not limited to) application and system software, development tools, utilities.

**Status Accounting** - a comparison of configuration data stored in a configuration database to actual device configuration. Used to ensure that recorded configuration data matches actual device configuration.

**System Security Plan** - repository to document security information and controls (management, operational and technical) regarding an application system.

**System Utility Programs** - Tools that when misused can subvert system, access and application controls E.g. network sniffers, password crackers, port scanners, root kits and vulnerability assessment scanners.

**Systems documentation** - detailed information about a system's design specifications, its internal workings, and its functionality including schematics, architectures, data structures, procedures and authorization processes.

**Systems privileges** - permissions which allow the user to alter access rights and structures of information systems.

**Telework** - a working arrangement where employees work away from their official workplace for a portion of their regular work week (Flexible Work Options). (See: ad hoc telework)

**Third party** - includes external party and includes a person outside the direct reporting structure of the Information Owner or Information Custodian. E.g., an individual, a business or organization, personnel from another branch of government, or another level of government.

**Threat** - in the security context, any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin. (See: vulnerability and event).

**Trusted path** - See: secured path

**Two person access control** - a system of requiring the presence of two authorized persons to perform an action, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. For example, a locked cabinet or safe which has two locks requiring action by two persons, each with a unique key or code and which requires the presence of two persons to access or open.

**Uninterruptible power supply** - a backup power source for computers and computer networks to insure on-going operation in the event of a power failure.

**User** - all persons authorized to access the Commission's internal bcogc.local domain in any capacity including employees and contractors.

**User identifier** - is the unique personal identifier that is authorized to access the Commission's computer and information systems.

**Vulnerability** - in the security context, a weakness in security procedures, processes, or controls that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

**Wireless Local Area Network** - a Local Area Network that uses wireless transmission media, such as 802.11a/b/g/n or WiMax.

**Zone** - See: reception zone, restricted access operations zone, restricted access security zone.

ISSUANCE: Corporate Services Division  
Records Management/Information Technology

APPROVED: April 27, 2021

## 1.0 GENERAL

### 1.1 Background

The BC Oil and Gas Commission (Commission) is adopting Microsoft Office 365 (M365) as a communication, collaboration and working platform. M365 provides a new suite of tools for creating, accessing, and sharing information and creates new digital workspaces.

### 1.2 Purpose

The purpose of this policy is to set a standard for how the Commission will use the M365 applications and appropriately manage the information residing in them. The use of M365 tools must comply with our legislative and policy requirements relating to information management and confidentiality. This means records and information stored using an M365 application or service must be:

- Appropriately retained to adequately document Commission decisions.
- Actively managed throughout their lifecycle according to retention policy.
- Secured and managed to prevent inadvertent disclosures.
- Assessed for confidentiality and, when appropriate, protected as a confidential asset.
- Readily accessible for Freedom of Information (FOI) and eDiscovery requests.

M365 is a new digital platform for the Commission and the Province, and its suitability as a corporate recordkeeping system has not yet been fully assessed. As such, this policy is deemed interim in nature and may be subject to future revisions.

#### • Authorities

- [Information Management Act](#)
- [Interpretation Act](#)
- [CRO 01-2019 Documenting Government Decisions Directive](#)
- [Freedom of Information and Protection of Privacy Act \(FOIPPA\)](#)
- [Transitory Records \(Schedule 102901\)](#)
- [Oil and Gas Regulation Operational Records Classification System \(ORCS\)](#)
- [Administrative Records Classification System \(ARCS\)](#)
- [Human Resources ARCS Supplement](#)

#### • Applicability

This policy applies to all data, records and information stored in M365 applications.



- **Related Policy/Procedure**

This policy, in conjunction with the following, is part of the information governance framework in the Commission:

- [Information Management Policy](#)
- [Managing Confidential Information Guide](#)
- [Managing Email Guide](#)
- [Employee Code of Conduct and Ethics](#)
- [Information Security Policy](#)
- [Mobile Device Policy](#)
- [Use of IT Resources Policy](#)

## 2.0 **POLICY**

### 2.1 **Records and Information Management**

- Commission records and information must be consistently managed according to approved information schedules (i.e., ARCS/ORCS).
- Official records within M365 workspaces must be saved to an appropriate recordkeeping system (shared drives) to ensure Commission decisions are adequately documented and business continuity and operations are supported.
- Only transitory information may be destroyed at the discretion of the employee.

### 2.2 **Collaboration and Protecting Confidentiality**

When using M365, users must limit the sharing of sensitive or confidential information, (e.g., personal information).

- Confidential records and personal information must not be inappropriately shared in M365 workspaces. If sharing is necessary, ensure proper handling and protections are in place.
- Access to M365 workspaces will only be granted to appropriate users and groups, as determined by Team/Site Owners.
- Access permissions assigned to collaborative workspaces will be actively managed, and access will be updated in a timely manner when group composites change.
- External individuals will not be granted access to Commission M365 workspaces without prior approval by a member of the Leadership group. If permissions are granted, Team/Site owners must ensure the protection of any confidential or sensitive information in the shared environment.

### 2.3 **Freedom of Information and legal records searches (eDiscovery)**

Information in M365, like all Commission information, is subject to the Freedom of Information and Protection of Privacy Act (FOIPPA) or other legal obligations. When using M365, staff must be prepared to respond to Freedom of Information (FOI) and legal requests for records and information.

Upon notification of a FOI and/or legal discovery request, users must assist in the search and retrieval of responsive records from applicable M365 workspaces, within prescribed time allowances as requested by FOI or Legal Services branch.

- Employees must not delete responsive records or information stored within M365 workspaces, including that which may be considered transitory. It is unlawful to delete or destroy any transitory record that is the subject of a current FOI request, or is subject to a current or reasonably anticipated litigation discovery process.
- Temporary holds on M365 automated information deletions should be initiated for applicable M365 applications.
- Searches for responsive records must be conducted within all applicable M365 workspaces.

### 3.0 APPLICATION USAGE

#### 3.1 Teams

Teams workspace is to be used for transitory information only.

Teams is used for:

- Ad hoc informal conversations (chats) between two or more people.
- Department/branch communications.
- Project/committee/working groups.

Retention of chat messages:

- Ad hoc chat messages (outside of Teams Sites and Channels) are automatically deleted after 10 days.
- Department/branch conversations (within a Teams Site or Channel) are automatically deleted after three months.
- Project/committee/working group conversations (within Teams Sites or Channels) are kept for the duration of the project, then deleted.

Documenting decisions and capturing official information in Teams:

- Any official or critical information in Teams must be captured in the recordkeeping system.
- Team/Site Owners must confirm that all official material has been transferred to the recordkeeping system before a Team site will be deleted.

#### 3.2 OneDrive

OneDrive is similar to the F: drive, by providing a private workspace for individual use. It is intended for short-term storage of records being actively worked on, i.e., drafting and collaborating on new documents. OneDrive is not an appropriate repository for long-term storage and management of Commission records.

OneDrive workspace should only hold active records while being drafted, and transitory information.

- When a record is finalized or collaboration has completed, it should be moved to the recordkeeping system.
- Users/Supervisors must confirm any official material has been transferred to the recordkeeping system before a OneDrive account is closed/deleted.

Confidentiality and collaboration considerations:

- Care must be taken to ensure that security and permissions are closely managed for confidential information being shared for collaboration.

### 3.3 SharePoint

There are two main uses of SharePoint in M365. Teams uses SharePoint as the platform for sharing and collaborating on documents – each Teams SharePoint is specific only to that Team and intended for short-term use and collaborative purposes. An official SharePoint site can also be used as a broader communication tool or collaboration hub at a corporate level; content stored on such sites is typically accessed across the organization and referenced for a period of longer duration, i.e., corporate policies and planning documentation, etc.

**Teams SharePoint** is a workspace for transitory content.

- Official records created within this workspace must be moved out of the Teams environment and saved to the recordkeeping system.

**SharePoint sites outside of Teams** are typically retained for a longer duration; as such, content must be managed according to records lifecycles and retention rules.

- Initiation of a corporate SharePoint site will be done in accordance with Commission SharePoint standards.
- Site structure must align with approved information schedule classifications.
- The Commission will actively maintain documentation on the intended use, access, and permissions for every site.
- SharePoint sites may be used as a records repository provided the structure aligns with information schedule classifications.
- When a site is closed, all official records should be extracted from SharePoint and saved to the recordkeeping system.

### 3.4 Outlook

M365 connects to Exchange Online instead of Exchange onsite. This does not significantly change email functionality or email management requirements.

- Emails should be managed according to information schedule classification and retention rules.
- Official emails should be routinely moved to and retained in the recordkeeping system.
- Inactive mailboxes may not be deleted until the contents have been assessed and official records are retained in the recordkeeping system.

## 4.0 ROLES AND RESPONSIBILITIES

**Leadership is responsible for:**

- Leading the Commission in the appropriate usage of M365 tools.

**Teams/Site Owners are responsible for:**

- Assigning and managing permissions to Commission workspaces.
- Ensuring the site or group workspace is appropriately managed according to Commission policy throughout its duration.

- Ensuring official records are captured in the recordkeeping system before a site/channel/group mailbox is closed.

**Each employee is responsible for:**

- Understanding what constitutes an official record and what information is deemed transitory.
- Managing Commission records and information, throughout the lifecycle established in approved information schedules, as appropriate to each M365 application.
- Ensuring appropriate confidentiality measures are applied to records and information.
- Ensuring the privacy of individuals is protected and maintained when using M365 tools and applications.
- Coordinating and/or conducting records searches within M365 applications in response to an FOI and/or legal request (eDiscovery).

**APPROVAL:**



**Paul Jeakins**  
Commissioner,  
Chief Executive Officer



**Len Dawes**  
Executive Vice President,  
Chief Financial Officer



**Ken Paulson**  
Executive Vice President,  
Chief Operating Officer



**Mayka Kennedy**  
Executive Vice President,  
Chief Engineer



**Ines Piccinino**  
Executive Vice President,  
Legal and Regulatory Affairs



**Trevor Swan**  
Executive Vice President,  
Orphan & Liability Management

**Version Control:**

Document Created	Apr-21	Approved by Executive Team

## Appendix A: Definitions

- **Access:** the ability or opportunity to view, study or obtain a copy of the records of the Commission. FOIPPA provides the public with a right of access to records in the custody or under the control of a public body.
- **Classification:** the process of identifying records or information in accordance with an approved information schedule. This includes determination of the function and/or subject of a record and selection of the appropriate records classification.
- **Confidential Record/Information:** is information that, if compromised, could result in serious consequences for individuals, organizations, or government. Designating information as confidential depends on factors such as the value of the information, the source of the information, and the impacts of unauthorized use, disclosure, alteration, reproduction, loss, or destruction. Confidential information requires protection against unauthorized access or disclosure.
- **Outlook:** is Microsoft's email application in M365. It supports the creation and receipt of electronic mail communication.
- **Information Governance (IG):** is fundamental to good corporate governance. It provides a framework and foundation for the control and securement of corporate records and information. It relates to the activities, policies, processes, and technologies an organization applies to maximize the value of the information it holds, while minimizing the costs and risks associated with holding it. The Commission's M365 IG Policy identifies requirements and strategies for managing content and records throughout their lifecycle using the suite of tools. The focus is on being compliant with applicable legislation and policies and enabling employees to be more collaborative and productive.
- **Information Schedules:** govern how records are organized and managed. B.C. government and broader public sector organizations use information schedules to ensure records are kept for as long as required, identify records of enduring value for preservation and ensure others are routinely destroyed when they are no longer needed.
- **Leadership Group:** Commission employees with a designation of Executive Director or higher.
- **Lifecycle:** the lifespan of information from its creation or receipt and use, through to its final disposition: destruction, transfer to the government archives or alienation.
- **Official Record/Information:** a record that documents Commission activities and decisions and does not fit the criteria of transitory records.
- **OneDrive:** cloud-based storage provided to each employee for information and materials related to their work.
- **Personal Information:** is recorded information about an identifiable individual other than business contact information. Business contact information identifies an individual in a business, professional or official capacity, and can include their name, title, business address, business telephone number, business email or business fax number. Personal information typically includes an individual's name, home address, personal email address, personal telephone number, age, gender, marital or family status, any physical or mental descriptors, information about an individual's educational, financial, criminal or employment history, personal views or opinions, and photos where individuals are identifiable. A name is considered personal under FOIPPA when, combined with other personal

information, it reveals something personal about that individual. The context in which an individual's name appears determines whether it is personal information.

- **Records/Information Management:** is the systematic control of information from creation to storage and retrieval to dissemination, regardless of media or physical format.
- **Recordkeeping System:** a shared filing system in which records are captured, protected, retained, and destroyed in accordance with approved information schedules, and the integrity of the digital government information is ensured. A recordkeeping system, when used in conjunction with recorded policies and procedures, defined roles and responsibilities, and ongoing training, constitutes an appropriate system for managing Commission information. Currently the Commission's recordkeeping system consists of shared drive folders.
- **Record/Information:** is created, received, and maintained by an organization or person during business. This includes formats defined in the Interpretation Act and FOIPPA, which includes "information that is recorded or stored by any means whether graphic, electronic, mechanical or otherwise".
- **Responsive Records/Information:** all records or information that pertain to the wording and/or subject of an FOI or legal request and fit within the scope of an applicant's request. A record may be deemed responsive as a result of its creation date, its content or context, who created the record, etc.
- **Retention Rules/Schedule:** embedded in Information Schedules, retention schedules govern the life cycle of a record, or series of records, provide the length of time the record is to be retained and its final disposition - destruction or transfer to the government archives.
- **SharePoint Site:** a central repository within M365 for information, links and content which may relate to a specific group of users for a specified purpose, or as a communication "hub" for an organization. SharePoint integrates with the other M365 applications and services and is intended for communication and collaboration.
- **Team's Site (referred to as a Team within Teams):** a collaborative workspace that provides transitory chat messaging, audio/video conferencing, document and information sharing, and meeting recordings. Team sites interface with a variety of M365 applications including Outlook, and documents residing in OneDrive and SharePoint. Teams Sites are structured with Channels, which are dedicated to a purpose.
- **Teams Channels:** dedicated conversation and workspace within Teams sites, where a group of people, such as project teams, committees, working groups, departments, and branches can collaborate and communicate.
- **Teams Chats (ad-hoc):** transitory instant messaging for the purpose of informal communication between people outside of Teams channels.
- **Team/Site Owner:** a Commission employee assigned as the owner of a Team who can create Channels within their team and manage permissions for those Channels. Additionally, Team Owners can set up properties for the Team including Team name and adding apps.
- **Transitory Information:** information of temporary and/or low value that is needed for only a limited period in order to complete a routine action or prepare a subsequent record (e.g., a new version). Transitory records are not required to meet statutory obligations or to sustain administrative or operational functions.

- **Workspace:** a broadly used term referring to M365 digital platforms where we work with records and information, such as a Teams collaboration space, SharePoint site and/or OneDrive location.



# Program Charter

Digital Information Management Program

**DRAFT**

Information Systems & Technology  
October 2022





Program Charter – Digital Information Management Program

---

**Program Overview**

Section 13



## Program Charter – Digital Information Management Program

---

### Program Scope

Section 13



Program Charter – Digital Information Management Program

---

Section 13



Program Charter – Digital Information Management Program

---

Section 13

**Program Stakeholders – Commission**

Stakeholder	Program Interest / Expectations
Executive Committee	Assurance regarding objectives and efficacy of the DIM Program
Executive Vice President, People, <a href="#">Reconciliation, Strategy &amp;</a> Transformation Division	Realization and support of Program vision and objectives
Executive Director, Information Systems & Technology	Strategic direction and oversight, financial support



## Program Charter – Digital Information Management Program

Leadership Group	Support for Program objectives, DWI (SharePoint) projects and staff engagement/time investment
VP Leadership Committee (VLC)	Contract, funding review and approvals
Director, Architecture & Innovation / A&I SMEs, project support resources	DWI Strategic direction and oversight, Program/project guidance and technical support
DWI Steering Committee	Committee of program subject matter experts <del>experts</del> to provide recommendations/input and enable project delivery (Leads: ED, IST and Director, A&I)
Director, Records & Information Services	DIM Program Strategic direction and oversight, project guidance
Manager, Digital Information (DIM Program Manager)	Program and project lead, project management, compliance review, user support, change management, Program efficacy, policies/processes, reporting, contract management
Program Business Analyst	Program technical requirements and tasks to support M365 and SharePoint projects, solution sustainment, compliance
Director, Cybersecurity	Security expertise and guidance
Director, IT / IT SMEs, project support resources	Technical expertise, <del>guidance</del> guidance, and support
Director, IS	IS/BA technical support and expertise
Departmental Leads/Staff	DWI (SharePoint) project support and participation, adherence to meeting schedules, <del>task</del> tasks, and timelines

### Program Contributors – Contractors

Contracted Contributor	Program Contribution / Value
Gravity Union – Digital Transformation / ECM Consulting	Delivery of DWI projects (intranet rebuild and SharePoint site development). Transfer of knowledge and hands-on support to IST staff who will become accountable for maintaining and sustaining the “workplace” upon contract completion.
File IT Solutions – Records & Information Management Consulting	Facilitation and delivery of SharePoint prerequisite work through departmental shared drive records classification, <del>organization</del> organization, and de-duplication – focus on alignment/compliance with Commission records policy framework. Day-to-day project management and support provided by Manager, Digital Information.

**Commented [AD12]:** This needs to be updated to current contractor.

**Program Roles & Responsibilities**

	Executive Program Champion - Ines Piccinino	DWI Steering Committee	Program Sponsor – Ab Dosil	DWI Program Director (Architecture & Innovation) – Derek Mathews	RM Program Director (Records & Info Services) – Kathryn Smerchinsky	DIM Program Manager – Mahia Frost	Program Business Analyst – 2022/23 Business Planning	IST Program/Project Resources – As Assigned	Departments – Site Owners and Users	Contracted Service Providers – Gravity Union	Contracted Service Providers – File IT Solutions
Program vision, establishing Executive buy-in of Program value	AR		C	I	I	I					
Program vision, Championing amongst Leadership Group, Executive liaison, VLC liaison	I		AR	C	C	C					
Ensuring alignment to Strategic & Capital plans	I		AR	C	C	C				C	
Program leadership and planning to achieve vision & objectives	I		C	A	A	R				C	
DWI contract & budget management, reporting	I	I	A	AR	I	I				C	
Hiring and/or allocation of Program resources	I		C	AR	AR	R		I			
Project planning & management, reporting		I	I	A	A	R		I	I	C	C
RM contract & budget management, reporting			I	I	A	R					C
Contractor liaison			AR	AR	AR	AR				R	R
Project championing, communications, change management	I	I	C	C	C	R	R	I		C	C
Project task execution & delivery, RM subject matter expertise, M365 IT technical expertise		I	A	A	A	AR	R	C	I	C	C
Solution sustainment, subject matter expertise, user training, <del>supporting</del> supporting, and reinforcing change	I	I	A	A	AR	AR	R	C	I	C	C
Compliance with legislated requirements & processes, auditing		I	A	A	AR	AR	R	C	I	AR	AR



Program Charter – Digital Information Management Program

---

Section 13



## Program Charter – Digital Information Management Program

---

### Approval

This charter formally authorizes the new Digital Information Management (DIM) Program, based on the information outlined in this charter.

**Approved by:**

**Approval Date:**

### Revision History

Version	Description of updates
0.1	Consolidation of program concept into Program Charter
0.2	





# General Service Agreement

For Administration Purpose Only

Account No: 55510-215-000002

Solicitation No: Quoted

Contract No: 21524001

BETWEEN	AND
<b>British Columbia Energy Regulator</b> also referred to as "Regulator"	<b>FY Information Management Consulting</b> also referred to as the "Contractor"
(the "Regulator", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	8508 Betts Road Wardner, BC V0B 2J0
Phone number: 250.419.4400 Email: <a href="mailto:procurement@bc-er.ca">procurement@bc-er.ca</a>	Phone Number: 250.417.1229 Email: <a href="mailto:michelle@fyinformation.ca">michelle@fyinformation.ca</a>

THE BC ENERGY REGULATOR AND THE CONTRACTOR AGREE TO THE TERMS AND CONDITIONS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

**SCHEDULE A – list of Services:** Electronic Filing Structure Consultant (See Attached)

**Term: Start Date:** September 1, 2023

**End Date:** March 31, 2024

<b>SCHEDULE B - FEES AND EXPENSES:</b>	
Fees: \$ 25,000	Expenses: \$
Billing Date(s): <b>Monthly / Upon Invoice</b>	Maximum Amount: <b>\$ 25,000</b>

**SCHEDULE C - APPROVED SUBCONTRACTOR(S):**

N/A

**SCHEDULE D - INSURANCE:**

(See Attached)

**SCHEDULE E – PRIVACY PROTECTION:**

(See Attached)

**SCHEDULE F – ADDITIONAL TERMS:**

N/A

**SCHEDULE G – SECURITY:**

N/A

SIGNED AND DELIVERED on the 6 <sup>th</sup> day of September 2023 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the 1 <sup>st</sup> day of September 2023 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
Signature	Signature
<b>Mahia Frost</b>	<b>Michelle Barroca</b>
Print Name	Print Name

**READ TERMS ON THE FOLLOWING PAGES**

# TERMS OF GENERAL SERVICE AGREEMENT

## 1 DEFINITIONS

### General

In this Agreement, unless the context otherwise requires:

- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
- (b) "Incorporated Material" means any material in existence prior to the beginning of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
- (c) "Material" means the Produced Material and the Received Material;
- (d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced by the Contractor or a Subcontractor and includes the Incorporated Material;
- (e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Regulator or any other person;
- (f) "Services" means the services described in Schedule A;
- (g) "Subcontractor" means an individual identified in paragraph (a) or (b) of section 13.4; and
- (h) "Term" means the term of the Agreement described in Schedule A subject to that term ending earlier in accordance with this Agreement.

### Meaning of "record"

- 1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

## 2 SERVICES

### Provision of services

- 2.1 The Contractor must provide the Services in accordance with this Agreement.

### Term

- 2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

### Supply of various items

- 2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

### Standard of care

- 2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

### Standards in relation to persons performing Services

- 2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

### Instructions by the Regulator

- 2.6 The Regulator may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are executed.

### Confirmation of non-written instructions

- 2.7 If the Regulator provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Regulator in writing, which request the Regulator must comply with as soon as it is reasonably practicable to do so.

### Effectiveness of non-written instructions

- 2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

### Applicable laws

- 2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws

## 3 PAYMENT

### Fees and expenses

- 3.1 If the Contractor complies with this Agreement, then the Regulator must pay to the Contractor at the times and on the conditions set forth in Schedule B:

- (a) The fees described in that Schedule, and
- (b) The expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Regulator's judgment, are necessarily incurred by the Contractor in providing the Services.
- (c) any applicable taxes payable by the Regulator under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Regulator is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

### Statements of accounts

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Regulator a written statement of account in a form satisfactory to the Regulator upon completion of the Services or at other times described in Schedule B.

### Withholding of amounts

- 3.3 Without limiting section 9.1, the Regulator may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Regulator and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Regulator to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Regulator.

### Appropriation

- 3.4 The Regulator's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Regulator during which payment becomes due.

### Currency

- 3.5 Unless otherwise specified in this Agreement, all references to money are in Canadian dollars.

### Non-resident income tax

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Regulator may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

### Prohibition against committing money

- 3.7 Without limiting section 13.10 (a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Regulator to pay any money except as may be expressly provided for in this Agreement.

### Refunds of taxes

- 3.8 The Contractor must apply for and, immediately on receipt, remit to the Regulator any available refund, rebate or remission of federal or provincial tax or duty that the Regulator has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement.

## 4 REPRESENTATIONS AND WARRANTIES

- 4.1 As of the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Regulator as follows: except to the extent the Contractor has previously disclosed otherwise in writing to the Regulator,

- (a) All information, statements, documents and reports furnished or submitted by the Contractor to the Regulator in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,
- (b) The Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractor agreements in place and available to enable the Contractor to fully perform the Services, and
- (c) The Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and if the Contractor is not an individual,

Contractor Initials: \_\_\_\_\_



BC Energy Regulator (authorized initials): \_\_\_\_\_ CMF

## TERMS OF GENERAL SERVICE AGREEMENT

- (d) The Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and
- (e) This Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

### 5 PRIVACY, SECURITY AND CONFIDENTIALITY

#### Privacy

- 5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

#### Security

- 5.2 The Contractor must:
- (a) Make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, modification or disposal; and
  - (b) Comply with the Security Schedule attached as Schedule G.

#### Confidentiality

- 5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Regulator's prior written consent except:
- (a) As required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
  - (b) If it is information that is generally known to the public other than as a result of a breach of this Agreement; or
  - (c) If it is information in any Incorporated Material.

#### Public announcements

- 5.4 Any public announcement relating to this Agreement will be arranged by the Regulator and, if such consultation is reasonably practicable, after consultation with the Contractor.

#### Restrictions on promotion

- 5.5 The Contractor must not, without the prior written approval of the Regulator, refer for promotional purposes to the Regulator being a customer of the Contractor or the Regulator having entered into this Agreement.

### 6 MATERIAL AND INTELLECTUAL PROPERTY

#### Access to Material

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Regulator, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Regulator.

#### Ownership and delivery of Material

- 6.2 The Regulator exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Regulator immediately upon the Regulator's request.

#### Matters respecting intellectual property

- 6.3 The Regulator exclusively owns all intellectual property rights, including copyright, in:
- (a) Received Material that the Contractor receives from the Regulator; and
  - (b) Produced Material, other than any Incorporated Material.
- Upon the Regulator's request, the Contractor must deliver to the Regulator documents satisfactory to the Regulator that irrevocably waive in the Regulator's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Regulator of the copyright in the Produced Material, other than any Incorporated Material.

#### Rights in relation to Incorporated Material

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Regulator:
- (a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify and distribute that Incorporated Material; and
  - (b) the right to sublicense to third-parties the right to use, reproduce, modify and distribute that Incorporated Material.

### 7 RECORDS AND REPORTS

#### Work reporting

- 7.1 Upon the Regulator's request, the Contractor must fully inform the Regulator of all work done by the Contractor or a Subcontractor in connection with providing the Services.

#### Time and expense records

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Regulator. Unless otherwise stipulated in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement terminates.

### 8 AUDIT

- 8.1 In addition to any other rights of inspection the Regulator may have under statute or otherwise, the Regulator may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Regulator's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Regulator of the Regulator's rights under this section.

### 9 INDEMNITY AND INSURANCE

#### Indemnity

- 9.1 The Contractor must indemnify and save harmless the Regulator and the Regulator's employees and agents from any losses, claims, damages, actions, causes of action, costs and expenses that the Regulator or any of the Regulator's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, including any claim of infringement of third-party intellectual property rights, where the same or any of them are based upon, arise out of or occur, directly or indirectly, by reason of any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement, excepting always liability arising out of the independent acts or omissions of the Regulator and the Regulator's employees and agents.

#### Insurance

- 9.2 The Contractor must comply, if attached, with the Insurance Schedule D.

#### Workers compensation

- 9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

#### Personal optional protection

- 9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
- (a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
  - (b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

#### Evidence of coverage

- 9.5 Within 10 Business Days of being requested to do so by the Regulator, the Contractor must provide the Regulator with evidence of the Contractor's compliance with sections 9.3 and 9.4.

### 10 FORCE MAJEURE

#### Definitions relating to force majeure

- 10.1 In this section and sections 10.2 and 10.3:
- (a) "Event of Force Majeure" means one the following events:
    - (i) a natural disaster, fire, flood, storm, epidemic or power failure;
    - (ii) a war (declared and undeclared), insurrection or act of terrorism or piracy, a strike (including illegal work stoppage or slowdown) or lockout, or a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
  - (b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Contractor Initials:         

BC Energy Regulator (authorized initials):          CMF



## TERMS OF GENERAL SERVICE AGREEMENT

### Waiver

- 13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

### Modifications

- 13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

### Entire agreement

- 13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to the performance of the Services.

### Survival of certain provisions

- 13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely, even after this Agreement ends.

### Schedules

- 13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

### Independent contractor

- 13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:  
(a) An employee or partner of the Regulator; or  
(b) An agent of the Regulator except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

### Personnel not to be employees of Regulator

- 13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Regulator.

### Key Personnel

- 13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Regulator otherwise approves in writing, which approval must not be unreasonably withheld.

### Pertinent information

- 13.13 The Regulator must make available to the Contractor all information in the Regulator's possession which the Regulator considers pertinent to the performance of the Services.

### Conflict of interest

- 13.14 The Contractor must not provide any services to any person in circumstances which, in the Regulator's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Regulator under this Agreement.

### Time

- 13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

### Conflicts among provisions

- 13.16 Conflicts among provisions of this Agreement will be resolved as follows:  
(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and  
(b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

### Agreement not permit nor fetter

- 13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Regulator or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Regulator or its agencies of any statutory, prerogative, executive or legislative power or duty.

### Remainder not affected by invalidity

- 13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

### Further assurances

- 13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

### Additional terms

- 13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

### Governing law

- 13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

## 14 INTERPRETATION

- 14.1 In this Agreement:  
(a) ... "Includes" and "including" are not intended to be limiting;  
(b) ... Unless the context otherwise requires, references to sections by number are to sections of this Agreement;  
(c) ... The Contractor and the Regulator are referred to as "the parties" and each of them as a "party";  
(d) ... "Attached" means attached to this Agreement when used in relation to a schedule;  
(e) ... Unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;  
(f) ... The headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;  
(g) ... "Person" includes an individual, partnership, corporation or legal entity of any nature; and  
(h) ... Unless the context otherwise requires, words expressed in the singular include the plural and vice versa.

Contractor Initials: 

BC Energy Regulator (authorized initials): CMFCMF

This Schedule forms part of the agreement

**Contract No: 21524001**

## DESCRIPTION OF SERVICES

The Contractor will assist Regulator staff in the formation of folder structures and folder naming conventions for one branch with 4 departments, containing roughly 270,000 documents.

Using established project framework from previous shared drive organization projects as a foundation, the Contractor will be:

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions, when appropriate
- Moving folders and associated records to the new folder structure (with user acceptance/permission); outside of business hours when required, to avoid disruption to information access
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary
- Identifying folders/files eligible for disposition
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

The Contractor will provide user support, training and change management by:

- Effectively initiating electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training to staff on the use and maintenance of the new shared drive folder structure

## Reporting Requirements

- The Contractor will provide briefings, status updates/reports, and final results reports as requested
- The Contractor will maintain a current work plan and project schedule and provide updates as needed.

## TERMS

The term of this Agreement commences on September 1, 2023 and ends on March 31, 2024.

## KEY PERSONNEL

All notice to the Regulator will be sent to the Contract Manager:

Mahia Frost  
Director, Records and Information Services  
Mahia.Frost@bc-er.ca

Contractor Initials: \_\_\_\_\_



BC Energy Regulator (authorized initials): \_\_\_\_\_ CCMFMF

This Schedule forms part of the agreement.

**Contract No: 21524001**

1. Fees will be paid at an hourly rate of \$135 per hour for the term during which the Contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, and in no event will the fees payable to the Contractor in accordance with this paragraph exceed, in aggregate, \$25,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).
2. The Contractor should submit to the Regulator, monthly, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.
3. After receipt by the Regulator of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.
4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is \$25,000, plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: 

BC Energy Regulator (authorized initials): CMF

This Schedule forms part of the agreement.

**Contract No: 21524001**

**Insurance:**

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Regulator:
  - (a) Commercial General Liability in an amount not less than **\$2,000,000.00** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
    - (i) include the Regulator as an additional insured,
    - (ii) be endorsed to provide the Regulator with 30 days advance written notice of cancellation or material change, and
    - (iii) include a cross liability clause;
2. All insurance described in section 1 of this Schedule must:
  - (a) be primary; and
  - (b) not require the sharing of any loss by any insurer of the Regulator.
3. The Contractor must provide the Regulator with evidence of all required insurance as follows:
  - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Regulator evidence of all required insurance in the form of a completed Certificate of Insurance;
  - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Regulator within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
  - (c) despite paragraph (a) or (b) above, if requested by the Regulator at any time, the Contractor must provide to the Regulator certified copies of the required insurance policies.
4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: \_\_\_\_\_



BC Energy Regulator (authorized initials): CMF



This Schedule forms part of the agreement.

**Contract No: 21524001**

**Definitions**

1. In this Schedule,
  - (a) **"Act"** means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
  - (b) **"contact information"** means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
  - (c) **"personal information"** means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Regulator and the Contractor dealing with the same subject matter as the Agreement.

**Purpose**

2. The purpose of this Schedule is to:
  - (a) enable the Regulator to comply with its statutory obligations under the Act with respect to personal information; and
  - (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

**Collection of personal information**

3. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
  - (a) the purpose for collecting it;
  - (b) the legal authority for collecting it; and
  - (c) the title, business address and business telephone number of the person designated by the Regulator to answer questions about the Contractor's collection of personal information.

**Accuracy of personal information**

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Regulator to make a decision that directly affects the individual the information is about.

**Requests for access to personal information**

7. If the Contractor receives a request for access to personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator unless the Agreement expressly requires the Contractor to provide such access and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

**Correction of personal information**

8. Within 5 business days of receiving a written direction from the Regulator to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
9. When issuing a written direction under section 8, the Regulator must advise the Contractor of the date the correction request to which the direction relates was received by the Regulator in order that the Contractor may comply with section 10.
10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Regulator, the Contractor disclosed the information being corrected or annotated.
11. If the Contractor receives a request for correction of personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

**Protection of personal information**

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Contractor Initials: 

BC Energy Regulator (authorized initials): CMF

This Schedule forms part of the agreement.

**Contract No: 21524001**

**Storage and access to personal information**

13. Unless the Regulator otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

**Retention of personal information**

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Regulator in writing to dispose of it or deliver it as specified in the direction.

**Use of personal information**

15. Unless the Regulator otherwise directs in writing, the Contractor may only use personal information if that use is:  
(a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and  
(b) in accordance with section 13.

**Disclosure of personal information**

16. Unless the Regulator otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Regulator if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
17. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

**Inspection of personal information**

18. In addition to any other rights of inspection the Regulator may have under the Agreement or under statute, the Regulator may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

**Compliance with the Act and directions**

19. The Contractor must in relation to personal information comply with:  
(a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the Commissioner under the Act; and  
(b) any direction given by the Regulator under this Schedule.
20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

**Notice of non-compliance**

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Regulator of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

**Termination of Agreement**

22. In addition to any other rights of termination which the Regulator may have under the Agreement or otherwise at law, the Regulator may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

**Interpretation**

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
26. If a provision of the Agreement (including any direction given by the Regulator under this Schedule) conflicts with a requirement of the Act or an applicable order of the Commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Contractor Initials: \_\_\_\_\_



BC Energy Regulator (authorized initials): \_\_\_\_\_ CMF



# General Service Agreement

For Administration Purpose Only

Account No: 55510-215-000002

Solicitation No: Quoted

Contract No: 21525001

BETWEEN	AND
<b>British Columbia Energy Regulator</b> also referred to as "Regulator"	<b>FY Information Management Consulting</b> also referred to as the "Contractor"
(the "Regulator", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	8508 Betts Road Wardner, BC V0B 2J0
Phone number: 250.419.4400 Email: <a href="mailto:procurement@bc-er.ca">procurement@bc-er.ca</a>	Phone Number: 250.417.1229 Email: <a href="mailto:michelle@fyinformation.ca">michelle@fyinformation.ca</a>

THE BC ENERGY REGULATOR AND THE CONTRACTOR AGREE TO THE TERMS AND CONDITIONS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

**SCHEDULE A – list of Services:** Electronic Filing Structure Consultant (See Attached)

**Term: Start Date:** April 1, 2024

**End Date:** March 31, 2025

<b>SCHEDULE B - FEES AND EXPENSES:</b>	
Fees: \$ 75,000	Expenses: \$
Billing Date(s): <b>Monthly / Upon Invoice</b>	Maximum Amount: <b>\$ 75,000</b>

**SCHEDULE C - APPROVED SUBCONTRACTOR(S):**

N/A

**SCHEDULE D - INSURANCE:**

(See Attached)

**SCHEDULE E – PRIVACY PROTECTION:**



(See Attached)

**SCHEDULE F – ADDITIONAL TERMS:**

N/A

**SCHEDULE G – SECURITY:**

N/A

SIGNED AND DELIVERED on the <u>2nd</u> day of April 2024 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the <u>2nd</u> day of April 2024 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
<b>Mahia Frost</b>	<b>Michelle Barroca</b>
Print Name	Print Name

**READ TERMS ON THE FOLLOWING PAGES**

# TERMS OF GENERAL SERVICE AGREEMENT

## 1 DEFINITIONS

### General

In this Agreement, unless the context otherwise requires:

- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
- (b) "Incorporated Material" means any material in existence prior to the beginning of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
- (c) "Material" means the Produced Material and the Received Material;
- (d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced by the Contractor or a Subcontractor and includes the incorporated Material;
- (e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Regulator or any other person;
- (f) "Services" means the services described in Schedule A;
- (g) "Subcontractor" means an individual identified in paragraph (a) or (b) of section 13.4; and
- (h) "Term" means the term of the Agreement described in Schedule A subject to that term ending earlier in accordance with this Agreement.

### Meaning of "record"

- 1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

## 2 SERVICES

### Provision of services

- 2.1 The Contractor must provide the Services in accordance with this Agreement.

### Term

- 2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

### Supply of various items

- 2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

### Standard of care

- 2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

### Standards in relation to persons performing Services

- 2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

### Instructions by the Regulator

- 2.6 The Regulator may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are executed.

### Confirmation of non-written instructions

- 2.7 If the Regulator provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Regulator in writing, which request the Regulator must comply with as soon as it is reasonably practicable to do so.

### Effectiveness of non-written instructions

- 2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

### Applicable laws

- 2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

## 3 PAYMENT

### Fees and expenses

- 3.1 If the Contractor complies with this Agreement, then the Regulator must pay to the Contractor at the times and on the conditions set forth in Schedule B:

- (a) The fees described in that Schedule, and
- (b) The expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Regulator's judgment, are necessarily incurred by the Contractor in providing the Services.
- (c) any applicable taxes payable by the Regulator under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Regulator is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

### Statements of accounts

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Regulator a written statement of account in a form satisfactory to the Regulator upon completion of the Services or at other times described in Schedule B.

### Withholding of amounts

- 3.3 Without limiting section 9.1, the Regulator may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Regulator and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Regulator to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Regulator.

### Appropriation

- 3.4 The Regulator's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Regulator during which payment becomes due.

### Currency

- 3.5 Unless otherwise specified in this Agreement, all references to money are in Canadian dollars.

### Non-resident income tax

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Regulator may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

### Prohibition against committing money

- 3.7 Without limiting section 13.10 (a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Regulator to pay any money except as may be expressly provided for in this Agreement.

### Refunds of taxes

- 3.8 The Contractor must apply for and, immediately on receipt, remit to the Regulator any available refund, rebate or remission of federal or provincial tax or duty that the Regulator has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement.

## 4 REPRESENTATIONS AND WARRANTIES

- 4.1 As of the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Regulator as follows: except to the extent the Contractor has previously disclosed otherwise in writing to the Regulator,

- (a) All information, statements, documents and reports furnished or submitted by the Contractor to the Regulator in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct;
- (b) The Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractor agreements in place and available to enable the Contractor to fully perform the Services; and
- (c) The Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and if the Contractor is not an individual,

Contractor Initials: 

BC Energy Regulator (authorized initials): \_\_\_\_\_

## TERMS OF GENERAL SERVICE AGREEMENT

- (d) The Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and
- (e) This Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

### 5 PRIVACY, SECURITY AND CONFIDENTIALITY

#### Privacy

- 5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

#### Security

- 5.2 The Contractor must:
  - (a) Make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, modification or disposal; and
  - (b) Comply with the Security Schedule attached as Schedule G.

#### Confidentiality

- 5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Regulator's prior written consent except:
  - (a) As required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
  - (b) If it is information that is generally known to the public other than as a result of a breach of this Agreement; or
  - (c) If it is information in any Incorporated Material.

#### Public announcements

- 5.4 Any public announcement relating to this Agreement will be arranged by the Regulator and, if such consultation is reasonably practicable, after consultation with the Contractor.

#### Restrictions on promotion

- 5.5 The Contractor must not, without the prior written approval of the Regulator, refer for promotional purposes to the Regulator being a customer of the Contractor or the Regulator having entered into this Agreement.

### 6 MATERIAL AND INTELLECTUAL PROPERTY

#### Access to Material

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Regulator, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Regulator.

#### Ownership and delivery of Material

- 6.2 The Regulator exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Regulator immediately upon the Regulator's request.

#### Matters respecting intellectual property

- 6.3 The Regulator exclusively owns all intellectual property rights, including copyright, in:
  - (a) Received Material that the Contractor receives from the Regulator; and
  - (b) Produced Material, other than any Incorporated Material.Upon the Regulator's request, the Contractor must deliver to the Regulator documents satisfactory to the Regulator that irrevocably waive in the Regulator's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Regulator of the copyright in the Produced Material, other than any Incorporated Material.

#### Rights in relation to Incorporated Material

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Regulator:
  - (a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify and distribute that Incorporated Material; and
  - (b) the right to sublicense to third-parties the right to use, reproduce, modify and distribute that Incorporated Material.

### 7 RECORDS AND REPORTS

#### Work reporting

- 7.1 Upon the Regulator's request, the Contractor must fully inform the Regulator of all work done by the Contractor or a Subcontractor in connection with providing the Services.

#### Time and expense records

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Regulator. Unless otherwise stipulated in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement terminates.

### 8 AUDIT

- 8.1 In addition to any other rights of inspection the Regulator may have under statute or otherwise, the Regulator may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Regulator's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Regulator of the Regulator's rights under this section.

### 9 INDEMNITY AND INSURANCE

#### Indemnity

- 9.1 The Contractor must indemnify and save harmless the Regulator and the Regulator's employees and agents from any losses, claims, damages, actions, causes of action, costs and expenses that the Regulator or any of the Regulator's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, including any claim of infringement of third-party intellectual property rights, where the same or any of them are based upon, arise out of or occur, directly or indirectly, by reason of any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement, excepting always liability arising out of the independent acts or omissions of the Regulator and the Regulator's employees and agents.

#### Insurance

- 9.2 The Contractor must comply, if attached, with the Insurance Schedule D.

#### Workers compensation

- 9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

#### Personal optional protection

- 9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
  - (a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
  - (b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

#### Evidence of coverage

- 9.5 Within 10 Business Days of being requested to do so by the Regulator, the Contractor must provide the Regulator with evidence of the Contractor's compliance with sections 9.3 and 9.4.

### 10 FORCE MAJEURE

#### Definitions relating to force majeure

- 10.1 In this section and sections 10.2 and 10.3:
  - (a) "Event of Force Majeure" means one of the following events:
    - (i) a natural disaster, fire, flood, storm, epidemic or power failure;
    - (ii) a war (declared and undeclared), insurrection or act of terrorism or piracy, a strike (including illegal work stoppage or slowdown) or lockout, or a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
  - (b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Contractor Initials: 

BC Energy Regulator (authorized initials): \_\_\_\_\_

## TERMS OF GENERAL SERVICE AGREEMENT

### Consequence of Event of Force Majeure

- 10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

### Duties of Affected Party

- 10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

## 11 DEFAULT AND TERMINATION

### Definitions relating to default and termination

- 11.1 In this section and sections 11.2 to 11.4:

- (a) "Event of Default" means any of the following:
- (i) an Insolvency Event,
  - (ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
  - (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and
- (b) "Insolvency Event" means any of the following:
- (i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
  - (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency, a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
  - (iii) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
  - (iv) a receiver or receiver-manager is appointed for any of the Contractor's property, or
  - (v) the Contractor ceases, in the Regulator's reasonable opinion, to carry on business as a going concern.

### Regulator's options on default:

- 11.2 On the happening of an Event of Default, or at any time thereafter, the Regulator may, at its option, elect to do any one or more of the following:
- (a) By written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
  - (b) Pursue any remedy or take any other action available to it at law or in equity; or
  - (c) By written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

### Delay not a waiver

- 11.3 No failure or delay on the part of the Regulator to exercise its rights in relation to an Event of Default will constitute a waiver by the Regulator of such rights.

### Regulator's right to terminate other than for default

- 11.4 In addition to the Regulator's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Regulator may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

### Payment consequences of termination

- 11.5 Unless Schedule B otherwise provides, if the Regulator terminates this Agreement under section 11.4:
- (a) The Regulator must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Regulator's satisfaction before termination of this Agreement; and
  - (b) The Contractor must, within 30 days of such termination, repay to the Regulator any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Regulator has notified the Contractor in writing was not completed to the Regulator's satisfaction before termination of this Agreement.

### Discharge of liability

- 11.6 The payment by the Regulator of the amount described in section 11.5(a) discharges the Regulator from all liability to make payments to the Contractor under this Agreement.

### Notice in relation to Events of Default

- 11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Regulator of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

## 12 DISPUTE RESOLUTION

### Dispute resolution process

- 12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
- (a) The parties must initially attempt to resolve the dispute through collaborative negotiation;
  - (b) If the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the British Columbia Mediator Roster Society; and
  - (c) If the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Commercial Arbitration Act*.

### Location of arbitration or mediation

- 12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

### Costs of mediation or arbitration

- 12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

## 13 MISCELLANEOUS

### Delivery of notices

- 13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
- (a) By email to the addressee's email address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
  - (b) By hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
  - (c) By prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

### Change of address or email address

- 13.2 Either party may from time to time give notice to the other party of a substitute address or email address, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email address specified for the party giving the notice.

### Assignment

- 13.3 The Contractor must not assign any of the Contractor's rights under this Agreement without the Regulator's prior written consent.

### Subcontracting

- 13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Regulator's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
- (a) Any person retained by the Contractor to perform obligations under this Agreement; and
  - (b) Any person retained by a person described in paragraph (a) to perform those obligations.
- Fully complies with this Agreement in performing the subcontracted obligations.

Contractor Initials: 

BC Energy Regulator (authorized initials): \_\_\_\_\_

## TERMS OF GENERAL SERVICE AGREEMENT

### Waiver

- 13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

### Modifications

- 13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

### Entire agreement

- 13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to the performance of the Services.

### Survival of certain provisions

- 13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely, even after this Agreement ends.

### Schedules

- 13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

### Independent contractor

- 13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:  
(a) An employee or partner of the Regulator; or  
(b) An agent of the Regulator except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

### Personnel not to be employees of Regulator

- 13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Regulator.

### Key Personnel

- 13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Regulator otherwise approves in writing, which approval must not be unreasonably withheld.

### Pertinent information

- 13.13 The Regulator must make available to the Contractor all information in the Regulator's possession which the Regulator considers pertinent to the performance of the Services.

### Conflict of interest

- 13.14 The Contractor must not provide any services to any person in circumstances which, in the Regulator's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Regulator under this Agreement.

### Time

- 13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

### Conflicts among provisions

- 13.16 Conflicts among provisions of this Agreement will be resolved as follows:  
(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and  
(b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

### Agreement not permit nor fetter

- 13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Regulator or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Regulator or its agencies of any statutory, prerogative, executive or legislative power or duty.

### Remainder not affected by invalidity

- 13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

### Further assurances

- 13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

### Additional terms

- 13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

### Governing law

- 13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

## 14 INTERPRETATION

- 14.1 In this Agreement:  
(a) ... "Includes" and "including" are not intended to be limiting;  
(b) ... Unless the context otherwise requires, references to sections by number are to sections of this Agreement;  
(c) ... The Contractor and the Regulator are referred to as "the parties" and each of them as a "party";  
(d) ... "Attached" means attached to this Agreement when used in relation to a schedule;  
(e) ... Unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;  
(f) ... The headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;  
(g) ... "Person" includes an individual, partnership, corporation or legal entity of any nature; and  
(h) ... Unless the context otherwise requires, words expressed in the singular include the plural and vice versa.

Contractor Initials: \_\_\_\_\_



BC Energy Regulator (authorized initials): \_\_\_\_\_

This Schedule forms part of the agreement

Contract No: 21525001

## DESCRIPTION OF SERVICES

The Contractor will assist Regulator staff in the formation of centralized shared drive folder structures which align to Regulator standards.

Using established project framework from previous shared drive organization projects as a foundation, the Contractor will be:

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions, when appropriate
- Moving folders and associated records to the new folder structure (with user acceptance/permission); outside of business hours when required to avoid disruption to information access
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary
- Identifying folders/files eligible for disposition and readying them for disposition by centralizing into one place
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

The Contractor will provide user support, training and change management by:

- Effectively initiating electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training to staff on the use and maintenance of the new shared drive folder structure

## Reporting Requirements

- The Contractor will provide briefings, status updates/reports, and final results reports as requested
- The Contractor will maintain a current work plan and project schedule and provide updates as needed.

## TERMS

The term of this Agreement commences on April 1, 2024 and ends on March 31, 2025. The Regulator, in its sole discretion, may renew this contract annually until March 31, 2027.

## KEY PERSONNEL

All notice to the Regulator will be sent to the Contract Manager:

Mahia Frost  
Director, Records and Information Services  
Mahia.Frost@bc-er.ca

Contractor Initials: 

BC Energy Regulator (authorized initials): \_\_\_\_\_



**SCHEDULE B  
Fees and Expenses**

This Schedule forms part of the agreement.

**Contract No: 21525001**

1. Fees will be paid at an hourly rate of \$135 per hour for the term during which the Contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, and in no event will the fees payable to the Contractor in accordance with this paragraph exceed, in aggregate, \$75,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).
2. The Contractor should submit to the Regulator, monthly, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.
3. After receipt by the Regulator of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.
4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is \$75,000, plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: 

BC Energy Regulator (authorized initials): \_\_\_\_\_

This Schedule forms part of the agreement.

**Contract No: 21525001**

**Insurance:**

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Regulator:
  - (a) Commercial General Liability in an amount not less than **\$2,000,000.00** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
    - (i) include the Regulator as an additional insured,
    - (ii) be endorsed to provide the Regulator with 30 days advance written notice of cancellation or material change, and
    - (iii) include a cross liability clause;
2. All insurance described in section 1 of this Schedule must:
  - (a) be primary; and
  - (b) not require the sharing of any loss by any insurer of the Regulator.
3. The Contractor must provide the Regulator with evidence of all required insurance as follows:
  - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Regulator evidence of all required insurance in the form of a completed Certificate of Insurance;
  - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Regulator within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
  - (c) despite paragraph (a) or (b) above, if requested by the Regulator at any time, the Contractor must provide to the Regulator certified copies of the required insurance policies.
4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: \_\_\_\_\_



BC Energy Regulator (authorized initials): \_\_\_\_\_

This Schedule forms part of the agreement.

**Contract No: 21525001**

**Definitions**

1. In this Schedule,
  - (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
  - (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
  - (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Regulator and the Contractor dealing with the same subject matter as the Agreement.

**Purpose**

2. The purpose of this Schedule is to:
  - (a) enable the Regulator to comply with its statutory obligations under the Act with respect to personal information; and
  - (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

**Collection of personal information**

3. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
  - (a) the purpose for collecting it;
  - (b) the legal authority for collecting it; and
  - (c) the title, business address and business telephone number of the person designated by the Regulator to answer questions about the Contractor's collection of personal information.

**Accuracy of personal information**

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Regulator to make a decision that directly affects the individual the information is about.

**Requests for access to personal information**

7. If the Contractor receives a request for access to personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator unless the Agreement expressly requires the Contractor to provide such access and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

**Correction of personal information**

8. Within 5 business days of receiving a written direction from the Regulator to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
9. When issuing a written direction under section 8, the Regulator must advise the Contractor of the date the correction request to which the direction relates was received by the Regulator in order that the Contractor may comply with section 10.
10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Regulator, the Contractor disclosed the information being corrected or annotated.
11. If the Contractor receives a request for correction of personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

**Protection of personal information**

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Contractor Initials: 

BC Energy Regulator (authorized initials): \_\_\_\_\_

This Schedule forms part of the agreement.

**Contract No: 21525001**

**Storage and access to personal information**

13. Unless the Regulator otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

**Retention of personal information**

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Regulator in writing to dispose of it or deliver it as specified in the direction.

**Use of personal information**

15. Unless the Regulator otherwise directs in writing, the Contractor may only use personal information if that use is:
- (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
  - (b) in accordance with section 13.

**Disclosure of personal information**

16. Unless the Regulator otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Regulator if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
17. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

**Inspection of personal information**

18. In addition to any other rights of inspection the Regulator may have under the Agreement or under statute, the Regulator may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

**Compliance with the Act and directions**

19. The Contractor must in relation to personal information comply with:
- (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the Commissioner under the Act; and
  - (b) any direction given by the Regulator under this Schedule.
20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

**Notice of non-compliance**

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Regulator of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

**Termination of Agreement**

22. In addition to any other rights of termination which the Regulator may have under the Agreement or otherwise at law, the Regulator may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

**Interpretation**

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
26. If a provision of the Agreement (including any direction given by the Regulator under this Schedule) conflicts with a requirement of the Act or an applicable order of the Commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Contractor Initials: 

BC Energy Regulator (authorized initials): \_\_\_\_\_



# General Service Agreement

For Administration Purpose Only

Account No: 55510-251-000003

Solicitation No: 25120001

Contract No: 25122001

<b>BETWEEN</b>	<b>AND</b>
<b>Oil and Gas Commission</b> also referred to as "Commission"	<b>File IT Solutions</b> also referred to as the "Contractor"
(the "Commission", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	810 Shamrock Street Victoria, BC V8X 2V1
Phone number: 250.419.4487	Phone Number: 250.386.3487
Email: <a href="mailto:Kathryn.Smerechinskiy@bcogc.ca">Kathryn.Smerechinskiy@bcogc.ca</a>	Email: <a href="mailto:Laurie.Phillips@fileitsolutions.com">Laurie.Phillips@fileitsolutions.com</a>

THE OIL AND GAS COMMISSION AND THE CONTRACTOR AGREE TO THE TERMS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

**SCHEDULE A – list of Services:** ARCS / ORCS Filing Structure Development (See attached)

**Term: Start Date:** April 19, 2021

**End Date:** March 31, 2022

<b>SCHEDULE B - FEES AND EXPENSES:</b>	
Fees: \$ 55 per hour	Expenses: \$ N/A
Billing Date(s): <b>Upon Invoice</b>	Maximum Amount: <b>\$ 75,000</b>

**SCHEDULE C - APPROVED SUBCONTRACTOR(S):** See attached.

**SCHEDULE D - INSURANCE:** See attached.

**SCHEDULE E – PRIVACY PROTECTION:** See attached.

**SCHEDULE F – ADDITIONAL TERMS:** N/A

**SCHEDULE G – SECURITY:** See attached.

SIGNED AND DELIVERED on the <u>25<sup>th</sup></u> day of March 2021 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the <u>25<sup>th</sup></u> day of March 2021 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
<b>Kathryn Smerechinskiy</b>	<b>Laurie Phillips</b>
Print Name	Print Name

**READ TERMS ON THE FOLLOWING PAGES**

# TERMS OF GENERAL SERVICE AGREEMENT

## 1 DEFINITIONS

### General

In this Agreement, unless the context otherwise requires:

- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
- (b) "Incorporated Material" means any material in existence prior to the beginning of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
- (c) "Material" means the Produced Material and the Received Material;
- (d) "Produced Material" means records, software and other material, whether complete or not, that as a result of this Agreement, are produced by the Contractor or a Subcontractor and includes the Incorporated Material;
- (e) "Received Material" means records, software and other material, whether complete or not, that as a result of this Agreement, are received by the Contractor or a Subcontractor from the Commission or any other person;
- (f) "Services" means the services described in Schedule A;
- (g) "Subcontractor" means an individual identified in paragraph (a) or (b) of section 13.4, and
- (h) "Term" means the term of the Agreement described in Schedule A subject to that term ending earlier in accordance with this Agreement.

### Meaning of "record"

- 1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

## 2 SERVICES

### Provision of services

- 2.1 The Contractor must provide the Services in accordance with this Agreement.

### Term

- 2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

### Supply of various items

- 2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

### Standard of care

- 2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

### Standards in relation to persons performing Services

- 2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

### Instructions by Commission

- 2.6 The Commission may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are executed.

### Confirmation of non-written instructions

- 2.7 If the Commission provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Commission in writing, which request the Commission must comply with as soon as it is reasonably practicable to do so.

### Effectiveness of non-written instructions

- 2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

### Applicable laws

- 2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

## 3 PAYMENT

### Fees and expenses

- 3.1 If the Contractor complies with this Agreement, then the Commission must pay to the Contractor at the times and on the conditions set forth in Schedule B:

- (a) The fees described in that Schedule, and
- (b) The expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and in the Commission's judgment, are necessarily incurred by the Contractor in providing the Services.
- (c) any applicable taxes payable by the Commission under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Commission is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

### Statements of accounts

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Commission a written statement of account in a form satisfactory to the Commission upon completion of the Services or at other times described in Schedule B.

### Withholding of amounts

- 3.3 Without limiting section 9.1, the Commission may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Commission and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Commission to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Commission.

### Appropriation

- 3.4 The Commission's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Commission during which payment becomes due.

### Currency

- 3.5 Unless otherwise specified in this Agreement, all references to money are in Canadian dollars.

### Non-resident income tax

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Commission may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

### Prohibition against commingling money

- 3.7 Without limiting section 13.10 (a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Commission to pay any money except as may be expressly provided for in this Agreement.

### Refunds of taxes

- 3.8 The Contractor must apply for and, immediately on receipt, remit to the Commission any available refund, rebate or remission of federal or provincial tax or duty that the Commission has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement.

## 4 REPRESENTATIONS AND WARRANTIES

- 4.1 As of the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Commission as follows: except to the extent the Contractor has previously disclosed otherwise in writing to the Commission,

- (a) All information, statements, documents and reports furnished or submitted by the Contractor to the Commission in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct;
- (b) The Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractor agreements in place and available to enable the Contractor to fully perform the Services; and
- (c) The Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and if the Contractor is not an individual,

Contractor Initials: 

Oil and Gas Commission (authorized initials): \_\_\_\_\_

## TERMS OF GENERAL SERVICE AGREEMENT

- (d) The Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor; and
- (e) This Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

### 5 PRIVACY, SECURITY AND CONFIDENTIALITY

#### Privacy

- 5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

#### Security

- 5.2 The Contractor must:
- Make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, modification or disposal; and
  - Comply with the Security Schedule attached as Schedule G.

#### Confidentiality

- 5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Commission's prior written consent except:
- As required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
  - If it is information that is generally known to the public other than as a result of a breach of this Agreement; or
  - If it is information in any Incorporated Material.

#### Public announcements

- 5.4 Any public announcement relating to this Agreement will be arranged by the Commission and, if such consultation is reasonably practicable, after consultation with the Contractor.

#### Restrictions on promotion

- 5.5 The Contractor must not, without the prior written approval of the Commission, refer for promotional purposes to the Commission being a customer of the Contractor or the Commission having entered into this Agreement.

### 6 MATERIAL AND INTELLECTUAL PROPERTY

#### Access to Material

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Commission, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Commission.

#### Ownership and delivery of Material

- 6.2 The Commission exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Commission immediately upon the Commission's request.

#### Matters respecting intellectual property

- 6.3 The Commission exclusively owns all intellectual property rights, including copyright, in:
- Received Material that the Contractor receives from the Commission; and
  - Produced Material, other than any Incorporated Material.
- Upon the Commission's request, the Contractor must deliver to the Commission documents satisfactory to the Commission that irrevocably waive in the Commission's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Commission of the copyright in the Produced Material, other than any Incorporated Material.

#### Rights in relation to Incorporated Material

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Commission:
- a non-exclusive perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify and distribute that Incorporated Material; and
  - the right to sublicense to third parties the right to use, reproduce, modify and distribute that Incorporated Material.

### 7 RECORDS AND REPORTS

#### Work reporting

- 7.1 Upon the Commission's request, the Contractor must fully inform the Commission of all work done by the Contractor or a Subcontractor in connection with providing the Services.

#### Time and expense records

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Commission. Unless otherwise stipulated in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement terminates.

### 8 AUDIT

- 8.1 In addition to any other rights of inspection the Commission may have under statute or otherwise, the Commission may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Commission of the Commission's rights under this section.

### 9 INDEMNITY AND INSURANCE

#### Indemnity

- 9.1 The Contractor must indemnify and save harmless the Commission and the Commission's employees and agents from any losses, claims, damages, actions, causes of action, costs and expenses that the Commission or any of the Commission's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, including any claim of infringement of third-party intellectual property rights, where the same or any of them are based upon, arise out of or occur, directly or indirectly, by reason of any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement, excepting always liability arising out of the independent acts or omissions of the Commission and the Commission's employees and agents.

#### Insurance

- 9.2 The Contractor must comply, if attached, with the insurance Schedule D.

#### Workers compensation

- 9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

#### Personal optional protection

- 9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
- the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
  - such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

#### Evidence of coverage

- 9.5 Within 10 Business Days of being requested to do so by the Commission, the Contractor must provide the Commission with evidence of the Contractor's compliance with sections 9.3 and 9.4.

### 10 FORCE MAJEURE

#### Definitions relating to force majeure

- 10.1 In this section and sections 10.2 and 10.3:
- "Event of Force Majeure" means one of the following events:
    - a natural disaster, fire, flood, storm, epidemic or power failure;
    - a war (declared and undeclared), insurrection or act of terrorism or piracy, a strike (including illegal work stoppage or slowdown) or lockout, or a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
  - "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Contractor Initials: XP

Oil and Gas Commission (authorized initials): \_\_\_\_\_

**TERMS OF GENERAL SERVICE AGREEMENT**

Consequence of Event of Force Majeure

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

Duties of Affected Party

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

**11 DEFAULT AND TERMINATION**

Definitions relating to default and termination

11.1 In this section and sections 11.2 to 11.4:  
(a) "Event of Default" means any of the following:  
(i) an Insolvency Event,  
(ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or  
(iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and  
(b) "Insolvency Event" means any of the following:  
(i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up;  
(ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency, a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor;  
(iii) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada);  
(iv) a receiver or receiver-manager is appointed for any of the Contractor's property, or  
(v) the Contractor ceases, in the Commission's reasonable opinion, to carry on business as a going concern.

Commission's options on default

11.2 On the happening of an Event of Default, or at any time thereafter, the Commission may, at its option, elect to do any one or more of the following:  
(a) By written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;  
(b) Pursue any remedy or take any other action available to it at law or in equity; or  
(c) By written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

Delay not a waiver

11.3 No failure or delay on the part of the Commission to exercise its rights in relation to an Event of Default will constitute a waiver by the Commission of such rights.

Commission's right to terminate other than for default

11.4 In addition to the Commission's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Commission may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

Payment consequences of termination

11.5 Unless Schedule B otherwise provides, if the Commission terminates this Agreement under section 11.4:  
(a) The Commission must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Commission's satisfaction before termination of this Agreement; and  
(b) The Contractor must, within 30 days of such termination, repay to the Commission any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Commission has notified the Contractor in writing was not completed to the Commission's satisfaction before termination of this Agreement.

Discharge of liability

11.6 The payment by the Commission of the amount described in section 11.5(a) discharges the Commission from all liability to make payments to the Contractor under this Agreement.

Notice in relation to Events of Default

11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Commission of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

**12 DISPUTE RESOLUTION**

Dispute resolution process

12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:  
(a) The parties must initially attempt to resolve the dispute through collaborative negotiation;  
(b) If the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the British Columbia Mediator Roster Society; and  
(c) If the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Commercial Arbitration Act*.

Location of arbitration or mediation

12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

Costs of mediation or arbitration

12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

**13 MISCELLANEOUS**

Delivery of notices

13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:  
(a) By email to the addressee's email address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;  
(b) By hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or  
(c) By prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

Change of address or email address

13.2 Either party may from time to time give notice to the other party of a substitute address or email address, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email address specified for the party giving the notice.

Assignment

13.3 The Contractor must not assign any of the Contractor's rights under this Agreement without the Commission's prior written consent.

Subcontracting

13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Commission's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:  
(a) Any person retained by the Contractor to perform obligations under this Agreement; and  
(b) Any person retained by a person described in paragraph (a) to perform those obligations,  
Fully complies with this Agreement in performing the subcontracted obligations.

Contractor Initials: 

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## TERMS OF GENERAL SERVICE AGREEMENT

### Waiver

13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

### Modifications

13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

### Entire agreement

13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to the performance of the Services.

### Survival of certain provisions

13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.4, 7.1, 7.2, 8.1, 9.1, 9.2, 9.5, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely, even after this Agreement ends.

### Schedules

13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

### Independent contractor

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:  
(a) An employee or partner of the Commission; or  
(b) An agent of the Commission except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

### Personnel not to be employees of Commission

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Commission.

### Key Personnel

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Commission otherwise approves in writing, which approval must not be unreasonably withheld.

### Pertinent information

13.13 The Commission must make available to the Contractor all information in the Commission's possession which the Commission considers pertinent to the performance of the Services.

### Conflict of interest

13.14 The Contractor must not provide any services to any person in circumstances which, in the Commission's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Commission under this Agreement.

### Time

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

### Conflicts among provisions

13.16 Conflicts among provisions of this Agreement will be resolved as follows:  
(a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and  
(b) a provision in a schedule will prevail over any conflicting provision in a document attached to or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

### Agreement not permit nor fetter

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Commission or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Commission or its agencies of any statutory, prerogative, executive or legislative power or duty.

### Remainder not affected by invalidity

13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

### Further assurances

13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

### Additional terms

13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

### Governing law

13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

## 14 INTERPRETATION

- 14.1 In this Agreement:
- (a) ... "Includes" and "including" are not intended to be limiting;
  - (b) ... Unless the context otherwise requires, references to sections by number are to sections of this Agreement;
  - (c) ... The Contractor and the Commission are referred to as "the parties" and each of them as a "party";
  - (d) ... "Attached" means attached to this Agreement when used in relation to a schedule;
  - (e) ... Unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
  - (f) ... The headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
  - (g) ... "Person" includes an individual, partnership, corporation or legal entity of any nature; and
  - (h) ... Unless the context otherwise requires, words expressed in the singular include the plural and vice versa.

Contractor initials: 

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE A SERVICES

This Schedule forms part of the agreement

Contract No: 25122001

The Contractor will provide the following services:

### DESCRIPTION OF SERVICES

#### Outputs / Outcomes

##### Establishment of folder structures and folder naming conventions

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions
- Moving folders and associated records to the new folder structure (with user acceptance/permission)
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary
- Identifying folders/files eligible for disposition
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

##### User support, training and change management:

- Effectively initiating each electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training (formal or desk-side) to staff on the use and maintenance of the new shared drive folder structure

#### Reporting Requirements

- Providing briefings, status updates/reports, and final results reports as requested
- Maintaining statistics/metrics for project tracking and communication purposes
- Maintaining a current work plan and project schedule

### TERMS

The term of this Agreement commences on April 19, 2021 and ends on March 31, 2022.

### KEY PERSONNEL

All notice to the Commission will be sent to the Contract Manager:

**Kathryn Smerechinskiy**  
2950 Jutland Road  
Victoria, BC V8T 5K2  
250-419-4487

The Key Personnel of the Contractor are as follows:

- (a) Marion Villines

Contractor Initials: \_\_\_\_\_

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE B Fees and Expenses

This Schedule forms part of the agreement

Contract No: 25122001

1. Fees will be paid at an hourly/daily rate of: \$55 per hour/day (8 hrs = 1 day), for the term during which the Contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, and in no event will the fees payable to the Contractor in accordance with this paragraph exceed, in aggregate, \$75,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).
2. The Contractor should submit to the Commission, upon completion of the project, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.
3. After receipt by the Commission of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.
4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is \$75,000 plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: SP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



**SCHEDULE C**  
**Approved Sub-contractor**

This Schedule forms part of the agreement

Contract No: 25122001

The following sub-contractor(s) has been approved under this Agreement:

1. Marion Villines

Contractor Initials: MP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE D Insurance

This Schedule forms part of the agreement

Contract No: 25122001

### Insurance:

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Commission:
  - (a) Commercial General Liability in an amount not less than **\$2,000,000.00** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
    - (i) include the Commission as an additional insured,
    - (ii) be endorsed to provide the Commission with 30 days advance written notice of cancellation or material change, and
    - (iii) include a cross liability clause.
2. All insurance described in section 1 of this Schedule must:
  - (a) be primary; and
  - (b) not require the sharing of any loss by any insurer of the Commission.
3. The Contractor must provide the Commission with evidence of all required insurance as follows:
  - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Commission evidence of all required insurance in the form of a completed Certificate of Insurance;
  - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Commission within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
  - (c) despite paragraph (a) or (b) above, if requested by the Commission at any time, the Contractor must provide to the Commission certified copies of the required insurance policies.
4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: AP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE E Privacy Protection

This Schedule forms part of the agreement.

Contract No: 25122001

### Definitions

1. In this Schedule,
  - (a) "Act" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
  - (b) "contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
  - (c) "personal information" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Commission and the Contractor dealing with the same subject matter as the Agreement.

### Purpose

2. The purpose of this Schedule is to:
  - (a) enable the Commission to comply with its statutory obligations under the Act with respect to personal information; and
  - (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

### Collection of personal information

3. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
  - (a) the purpose for collecting it;
  - (b) the legal authority for collecting it; and
  - (c) the title, business address and business telephone number of the person designated by the Commission to answer questions about the Contractor's collection of personal information.

### Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Commission to make a decision that directly affects the individual the information is about.

### Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission unless the Agreement expressly requires the Contractor to provide such access and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

### Correction of personal information

8. Within 5 business days of receiving a written direction from the Commission to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
9. When issuing a written direction under section 8, the Commission must advise the Contractor of the date the correction request to which the direction relates was received by the Commission in order that the Contractor may comply with section 10.
10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Commission, the Contractor disclosed the information being corrected or annotated.
11. If the Contractor receives a request for correction of personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

### Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

### Storage and access to personal information

13. Unless the Commission otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Contractor Initials: LP

Oil and Gas Commission (authorized initials) \_\_\_\_\_



## SCHEDULE E Privacy Protection

This Schedule forms part of the agreement.

Contract No: 25122001

### Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Commission in writing to dispose of it or deliver it as specified in the direction.

### Use of personal information

15. Unless the Commission otherwise directs in writing, the Contractor may only use personal information if that use is:
- (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
  - (b) in accordance with section 13.

### Disclosure of personal information

16. Unless the Commission otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Commission if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
17. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

### Inspection of personal information

18. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

### Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
- (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
  - (b) any direction given by the Commission under this Schedule.
20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

### Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Commission of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

### Termination of Agreement

22. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

### Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
26. If a provision of the Agreement (including any direction given by the Commission under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

### Definitions

Contractor Initials: SP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE G Security

This Schedule forms part of the agreement.

Contract No: 25122001

1. In this Schedule,
  - a. "Equipment" means any equipment, including interconnected systems or subsystems of equipment, software and networks, used or to be used by the Contractor to provide the Services;
  - b. "Facilities" means any facilities at which the Contractor provides or is to provide the Services;
  - c. "Information" means information
    - i. in the Material, or
    - ii. accessed, produced or obtained by the Contractor (whether verbally, electronically or otherwise) as a result of the Agreement;
  - d. "Record" means a "record" as defined in the Interpretation Act;
  - e. "Sensitive Information" means
    - i. Information that is "personal information" as defined in the Freedom of Information and Protection of Privacy Act, or
    - ii. any other Information specified as "Sensitive Information" in Appendix G6, if attached; and
  - f. "Services Worker" means an individual involved in providing the Services for or on behalf of the Contractor and, for greater certainty, may include
    - i. the Contractor or a subcontractor if an individual, or
    - ii. an employee or volunteer of the Contractor or of a subcontractor.

### Schedule contains additional obligations

2. The obligations of the Contractor in this Schedule are in addition to any other obligations in the Agreement or the schedules attached to it relating to security including, without limitation, the obligations of the Contractor in the Privacy Protection Schedule, if attached.

### Services Worker confidentiality agreements

3. The Contractor must not permit a Services Worker who is an employee or volunteer of the Contractor to have access to Sensitive Information unless the Services Worker has first entered into a confidentiality agreement with the Contractor to keep Sensitive Information confidential on substantially similar terms as those that apply to the Contractor under the Agreement.

### Services Worker security screening

4. The Contractor may only permit a Services Worker who is an employee or a volunteer of the Contractor to have access to Sensitive Information or otherwise be involved in providing the Services if, after having subjected the Services Worker to the personnel security screening requirements and any additional requirements the Contractor may consider appropriate, the Contractor is satisfied that the Services Worker does not constitute an unreasonable security risk.

Contractor Initials: SP

Oil and Gas Commission (authorized initials): \_\_\_\_\_





## SCHEDULE G Security

This Schedule forms part of the agreement.

Contract No: 25122001

### Services Worker activity logging

5. Subject to section 6, the Contractor must create and maintain detailed Records logging the activities of all Service Workers in relation to:
  - a. their access to Sensitive Information; and
  - b. other matters specified by the Commission in writing for the purposes of this section.
6. The Records described in section 5 must be made and maintained in a manner, and contain information, specified in Appendix G2, if attached.

### Facilities and Equipment protection and access control

7. The Contractor must create, maintain and follow a documented process to:
  - a. protect Facilities and Equipment of the Contractor required by the Contractor to provide the Services from loss, damage or any other occurrence that may result in any of those Facilities and Equipment being unavailable when required to provide the Services; and
  - b. limit access to Facilities and Equipment of the Contractor
    - i. being used by the Contractor to provide the Services, or
    - ii. that may be used by someone to access Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons.
8. If the Commission makes available to the Contractor any Facilities or Equipment of the Commission for the use of the Contractor in providing the Services, the Contractor must comply with any policies and procedures provided to it by the Commission on acceptable use, protection of, and access to, such Facilities or Equipment.

### Sensitive Information access control

9. The Contractor must:
  - a. create, maintain and follow a documented process for limiting access to Sensitive Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons; and
  - b. comply with the information access control requirements set out in Appendix G3, if attached.

### Integrity of Information

10. The Contractor must:
  - a. create, maintain and follow a documented process for maintaining the integrity of Information while possessed or accessed by the Contractor; and
  - b. comply with the information integrity requirements set out in Appendix G4, if attached.
11. For the purposes of section 10, maintaining the integrity of Information means that, except to the extent expressly authorized by the Agreement or approved in writing by the Commission, the Information has:
  - a. remained as complete as when it was acquired or accessed by the Contractor; and
  - b. not been altered in any material respect.

Contractor Initials: RP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE G Security

This Schedule forms part of the agreement.

Contract No: 25122001

### Documentation of changes to processes

12. The Contractor must create and maintain detailed Records logging any changes it makes to the processes described in sections 7, 9 and 10.

### Notice of security breaches

13. If Contractor becomes aware that:
  - a. unauthorized access, collection, use, disclosure, alteration or disposal of Information or Records containing Information; or
  - b. unauthorized access to Facilities or Equipment has occurred or is likely to occur (whether or not related to a failure by the Contractor to comply with this Schedule or the Agreement), the Contractor must immediately notify the Commission of the particulars of that occurrence or likely occurrence. If the Contractor provides a notification under this section other than in writing, that notification must be confirmed in writing to the Commission as soon as it is reasonably practicable for the Contractor to do so.

### Review of security breaches

14. If the Commission decides to conduct a review of a matter described in section 13 (whether or not the matter came to the attention of the Commission as a result of a notification under section 13), the Contractor must, on the request of the Commission, participate in the review to the extent that it is reasonably practicable for the Contractor to do so.

### Retention of Records

15. Unless the Agreement otherwise specifies, the Contractor must retain all Records in the Contractor's possession that contain Information until directed by the Commission in writing to dispose of them or deliver them as specified in the direction.

### Storage of Records

16. Until disposed of or delivered in accordance with section 15, the Contractor must store any Records in the Contractor's possession that contain Information in accordance with the provisions of Appendix G5, if attached.

### Audit

17. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy:
  - a. any Records in the possession of the Contractor containing Information; or
  - b. any of the Contractor's Information management policies or processes (including the processes described in sections 7, 9 and 10 and the logs described in sections 5 and 12) relevant to the Contractor's compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to the exercise by the Commission of the Commission's rights under this section.

Contractor Initials: \_\_\_\_\_

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE G Security

This Schedule forms part of the agreement.

Contract No: 25122001

### Termination of Agreement

18. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

### Interpretation

19. In this Schedule, unless otherwise specified:
- a. references to sections are to sections of this Schedule; and
  - b. references to appendices are to the appendices attached to this Schedule.
20. Any reference to the "Contractor" in this Schedule includes any subcontractor retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors comply with this Schedule.
21. The appendices attached to this Schedule are part of this Schedule.
22. If there is a conflict between a provision in an appendix attached to this Schedule and any other provision of this Schedule, the provision in the appendix is inoperative to the extent of the conflict unless the appendix states that it operates despite a conflicting provision of this Schedule.
23. If there is a conflict between:
- a. a provision of the Agreement, this Schedule or an appendix attached to this Schedule; and
  - b. a documented process required by this Schedule to be created or maintained by the Contractor
- the provision of the Agreement, Schedule or appendix will prevail to the extent of the conflict.
24. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

Contractor Initials:     *AP*    

Oil and Gas Commission (authorized initials): \_\_\_\_\_



CONTRACT No. 25122001

CONTRACT AMENDMENT #2

THIS AMENDMENT MADE THIS 25<sup>th</sup> DAY OF MARCH 2022

BETWEEN:

OIL AND GAS COMMISSION (HEREIN CALLED THE "COMMISSION")  
OF THE FIRST PART

AND:

FILE IT SOLUTIONS (HEREIN CALLED THE "CONTRACTOR")  
OF THE SECOND PART

WITNESSETH THAT WHEREAS:

- A. The parties hereto entered into a General Services Agreement identified as Contract No. 25122001 (the "Agreement") for a term which initially commenced on April 19, 2021 and was scheduled to end on March 31, 2022;
- B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:

- 1. This amendment and renewal of the Agreement is made effective April 1, 2022.
- 2. The term of the contract is to be extended to March 2023. The term described in Schedule "A" is deleted and replaced with:  
  
The term of this Agreement commences on April 19, 2021 and is scheduled to end on March 31, 2023. The Commission has discretion to offer a one-year renewal of services at that time.
- 3. Maximum fees will increase by \$75,000 from \$75,000 to \$150,000. Schedule B, Clauses 1 and 4 will be deleted and replace with:
  - 1. Fees will be paid at an hourly rate of: \$55 per hour for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract and in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, \$150,000, exclusive of any applicable taxes.
  - 6. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is **\$150,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.
- 4. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the <u>29</u> day of March 2022 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the <u>25</u> day of March 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
<i>K. Smerechinskiy</i>	<i>Laurie Phillips</i>
Signature	Signature
<b>Kathryn Smerechinskiy</b>	<b>Laurie Phillips</b>
Print Name	Print Name



# General Service Agreement

For Administration Purpose Only

Account No: 55510-251-000003

Solicitation No: 25120001

Contract No: 25122001

<b>BETWEEN</b>	<b>AND</b>
<b>Oil and Gas Commission</b> also referred to as "Commission"	<b>File IT Solutions</b> also referred to as the "Contractor"
(the "Commission", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	810 Shamrock Street Victoria, BC V8X 2V1
Phone number: 250.419.4487	Phone Number: 250.386.3487
Email: <a href="mailto:Kathryn.Smerechinskiy@bcogc.ca">Kathryn.Smerechinskiy@bcogc.ca</a>	Email: <a href="mailto:Laurie.Phillips@fileitsolutions.com">Laurie.Phillips@fileitsolutions.com</a>

THE OIL AND GAS COMMISSION AND THE CONTRACTOR AGREE TO THE TERMS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

**SCHEDULE A – list of Services:** ARCS / ORCS Filing Structure Development (See attached)

**Term: Start Date:** April 19, 2021

**End Date:** March 31, 2022

<b>SCHEDULE B - FEES AND EXPENSES:</b>	
Fees: \$ 55 per hour	Expenses: \$ N/A
Billing Date(s): <b>Upon Invoice</b>	Maximum Amount: <b>\$ 75,000</b>

**SCHEDULE C - APPROVED SUBCONTRACTOR(S):** See attached.

**SCHEDULE D - INSURANCE:** See attached.

**SCHEDULE E – PRIVACY PROTECTION:** See attached.

**SCHEDULE F – ADDITIONAL TERMS:** N/A

**SCHEDULE G – SECURITY:** See attached.

SIGNED AND DELIVERED on the <u>25<sup>th</sup></u> day of March 2021 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the <u>25<sup>th</sup></u> day of March 2021 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
Signature	Signature
<b>Kathryn Smerechinskiy</b>	<b>Laurie Phillips</b>
Print Name	Print Name

**READ TERMS ON THE FOLLOWING PAGES**

# TERMS OF GENERAL SERVICE AGREEMENT

## 1 DEFINITIONS

### General

In this Agreement, unless the context otherwise requires:

- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
- (b) "Incorporated Material" means any material in existence prior to the beginning of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
- (c) "Material" means the Produced Material and the Received Material;
- (d) "Produced Material" means records, software and other material, whether complete or not, that as a result of this Agreement, are produced by the Contractor or a Subcontractor and includes the Incorporated Material;
- (e) "Received Material" means records, software and other material, whether complete or not, that as a result of this Agreement, are received by the Contractor or a Subcontractor from the Commission or any other person;
- (f) "Services" means the services described in Schedule A;
- (g) "Subcontractor" means an individual identified in paragraph (a) or (b) of section 13.4, and
- (h) "Term" means the term of the Agreement described in Schedule A subject to that term ending earlier in accordance with this Agreement.

### Meaning of "record"

- 1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

## 2 SERVICES

### Provision of services

- 2.1 The Contractor must provide the Services in accordance with this Agreement.

### Term

- 2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

### Supply of various items

- 2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

### Standard of care

- 2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

### Standards in relation to persons performing Services

- 2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

### Instructions by Commission

- 2.6 The Commission may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are executed.

### Confirmation of non-written instructions

- 2.7 If the Commission provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Commission in writing, which request the Commission must comply with as soon as it is reasonably practicable to do so.

### Effectiveness of non-written instructions

- 2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

### Applicable laws

- 2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

## 3 PAYMENT

### Fees and expenses

- 3.1 If the Contractor complies with this Agreement, then the Commission must pay to the Contractor at the times and on the conditions set forth in Schedule B:

- (a) The fees described in that Schedule, and
- (b) The expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and in the Commission's judgment, are necessarily incurred by the Contractor in providing the Services.
- (c) any applicable taxes payable by the Commission under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Commission is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

### Statements of accounts

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Commission a written statement of account in a form satisfactory to the Commission upon completion of the Services or at other times described in Schedule B.

### Withholding of amounts

- 3.3 Without limiting section 9.1, the Commission may withhold from any payment due to the Contractor an amount sufficient to indemnify, in whole or in part, the Commission and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Commission to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Commission.

### Appropriation

- 3.4 The Commission's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Commission during which payment becomes due.

### Currency

- 3.5 Unless otherwise specified in this Agreement, all references to money are in Canadian dollars.

### Non-resident income tax

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Commission may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

### Prohibition against commingling money

- 3.7 Without limiting section 13.10 (a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Commission to pay any money except as may be expressly provided for in this Agreement.

### Refunds of taxes

- 3.8 The Contractor must apply for and, immediately on receipt, remit to the Commission any available refund, rebate or remission of federal or provincial tax or duty that the Commission has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement.

## 4 REPRESENTATIONS AND WARRANTIES

- 4.1 As of the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Commission as follows: except to the extent the Contractor has previously disclosed otherwise in writing to the Commission,

- (a) All information, statements, documents and reports furnished or submitted by the Contractor to the Commission in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct;
- (b) The Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractor agreements in place and available to enable the Contractor to fully perform the Services; and
- (c) The Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and if the Contractor is not an individual,

Contractor Initials: 

Oil and Gas Commission (authorized initials): \_\_\_\_\_

## TERMS OF GENERAL SERVICE AGREEMENT

- (d) The Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor; and
- (e) This Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

### 5 PRIVACY, SECURITY AND CONFIDENTIALITY

#### Privacy

- 5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

#### Security

- 5.2 The Contractor must:
- Make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, modification or disposal; and
  - Comply with the Security Schedule attached as Schedule G.

#### Confidentiality

- 5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Commission's prior written consent except:
- As required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
  - If it is information that is generally known to the public other than as a result of a breach of this Agreement; or
  - If it is information in any Incorporated Material.

#### Public announcements

- 5.4 Any public announcement relating to this Agreement will be arranged by the Commission and, if such consultation is reasonably practicable, after consultation with the Contractor.

#### Restrictions on promotion

- 5.5 The Contractor must not, without the prior written approval of the Commission, refer for promotional purposes to the Commission being a customer of the Contractor or the Commission having entered into this Agreement.

### 6 MATERIAL AND INTELLECTUAL PROPERTY

#### Access to Material

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Commission, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Commission.

#### Ownership and delivery of Material

- 6.2 The Commission exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Commission immediately upon the Commission's request.

#### Matters respecting intellectual property

- 6.3 The Commission exclusively owns all intellectual property rights, including copyright, in:
- Received Material that the Contractor receives from the Commission; and
  - Produced Material, other than any Incorporated Material.
- Upon the Commission's request, the Contractor must deliver to the Commission documents satisfactory to the Commission that irrevocably waive in the Commission's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Commission of the copyright in the Produced Material, other than any Incorporated Material.

#### Rights in relation to Incorporated Material

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Commission:
- a non-exclusive perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify and distribute that Incorporated Material; and
  - the right to sublicense to third parties the right to use, reproduce, modify and distribute that Incorporated Material.

### 7 RECORDS AND REPORTS

#### Work reporting

- 7.1 Upon the Commission's request, the Contractor must fully inform the Commission of all work done by the Contractor or a Subcontractor in connection with providing the Services.

#### Time and expense records

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Commission. Unless otherwise stipulated in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement terminates.

### 8 AUDIT

- 8.1 In addition to any other rights of inspection the Commission may have under statute or otherwise, the Commission may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Commission of the Commission's rights under this section.

### 9 INDEMNITY AND INSURANCE

#### Indemnity

- 9.1 The Contractor must indemnify and save harmless the Commission and the Commission's employees and agents from any losses, claims, damages, actions, causes of action, costs and expenses that the Commission or any of the Commission's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, including any claim of infringement of third-party intellectual property rights, where the same or any of them are based upon, arise out of or occur, directly or indirectly, by reason of any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement, excepting always liability arising out of the independent acts or omissions of the Commission and the Commission's employees and agents.

#### Insurance

- 9.2 The Contractor must comply, if attached, with the insurance Schedule D.

#### Workers compensation

- 9.3 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

#### Personal optional protection

- 9.4 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
- the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
  - such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

#### Evidence of coverage

- 9.5 Within 10 Business Days of being requested to do so by the Commission, the Contractor must provide the Commission with evidence of the Contractor's compliance with sections 9.3 and 9.4.

### 10 FORCE MAJEURE

#### Definitions relating to force majeure

- 10.1 In this section and sections 10.2 and 10.3:
- "Event of Force Majeure" means one of the following events:
    - a natural disaster, fire, flood, storm, epidemic or power failure;
    - a war (declared and undeclared), insurrection or act of terrorism or piracy, a strike (including illegal work stoppage or slowdown) or lockout, or a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
  - "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

Contractor Initials: XP

Oil and Gas Commission (authorized initials): \_\_\_\_\_

**TERMS OF GENERAL SERVICE AGREEMENT**

**Consequence of Event of Force Majeure**

10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

**Duties of Affected Party**

10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

**11 DEFAULT AND TERMINATION**

**Definitions relating to default and termination**

11.1 In this section and sections 11.2 to 11.4:

- (a) "Event of Default" means any of the following:
  - (i) an Insolvency Event,
  - (ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
  - (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and
- (b) "Insolvency Event" means any of the following:
  - (i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
  - (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency, a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
  - (iii) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
  - (iv) a receiver or receiver-manager is appointed for any of the Contractor's property, or
  - (v) the Contractor ceases, in the Commission's reasonable opinion, to carry on business as a going concern.

**Commission's options on default**

11.2 On the happening of an Event of Default, or at any time thereafter, the Commission may, at its option, elect to do any one or more of the following:

- (a) By written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
- (b) Pursue any remedy or take any other action available to it at law or in equity; or
- (c) By written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

**Delay not a waiver**

11.3 No failure or delay on the part of the Commission to exercise its rights in relation to an Event of Default will constitute a waiver by the Commission of such rights.

**Commission's right to terminate other than for default**

11.4 In addition to the Commission's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Commission may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

**Payment consequences of termination**

11.5 Unless Schedule B otherwise provides, if the Commission terminates this Agreement under section 11.4:

- (a) The Commission must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Commission's satisfaction before termination of this Agreement; and
- (b) The Contractor must, within 30 days of such termination, repay to the Commission any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Commission has notified the Contractor in writing was not completed to the Commission's satisfaction before termination of this Agreement.

**Discharge of liability**

11.6 The payment by the Commission of the amount described in section 11.5(a) discharges the Commission from all liability to make payments to the Contractor under this Agreement.

**Notice in relation to Events of Default**

11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Commission of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

**12 DISPUTE RESOLUTION**

**Dispute resolution process**

12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:

- (a) The parties must initially attempt to resolve the dispute through collaborative negotiation;
- (b) If the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the British Columbia Mediator Roster Society; and
- (c) If the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Commercial Arbitration Act*.

**Location of arbitration or mediation**

12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

**Costs of mediation or arbitration**

12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a mediation or arbitration under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

**13 MISCELLANEOUS**

**Delivery of notices**

13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:

- (a) By email to the addressee's email address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
- (b) By hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
- (c) By prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

**Change of address or email address**

13.2 Either party may from time to time give notice to the other party of a substitute address or email address, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email address specified for the party giving the notice.

**Assignment**

13.3 The Contractor must not assign any of the Contractor's rights under this Agreement without the Commission's prior written consent.

**Subcontracting**

13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Commission's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:

- (a) Any person retained by the Contractor to perform obligations under this Agreement; and
- (b) Any person retained by a person described in paragraph (a) to perform those obligations;

Fully complies with this Agreement in performing the subcontracted obligations.

Contractor Initials: \_\_\_\_\_

Oil and Gas Commission (authorized initials): \_\_\_\_\_







## SCHEDULE A SERVICES

This Schedule forms part of the agreement

Contract No: 25122001

The Contractor will provide the following services:

### DESCRIPTION OF SERVICES

#### Outputs / Outcomes

##### Establishment of folder structures and folder naming conventions

- Developing accurate, standardized electronic folder structures based on Commission program records and business requirements, and applicable records schedules (ARCS/ORCS)
- Establishing and implementing standardized folder naming conventions
- Moving folders and associated records to the new folder structure (with user acceptance/permission)
- Identifying and removing transitory or duplicate records (clean-up), and other folders deemed necessary
- Identifying folders/files eligible for disposition
- Establishing a security matrix for the folders with established business rules related to configuration and necessary permissions

##### User support, training and change management:

- Effectively initiating each electronic filing project with program staff to ensure clear understanding of project scope and methodology, expectations of staff, and what support will be available
- Consulting with staff throughout the project to ensure their input results in a structure that is both intuitive and easy to follow
- Providing effective communications and guidance to ensure staff can locate records in a timely manner at any given point of the project (first point of contact)
- Educating staff to encourage transfer of any official records saved on personal drives to the new shared folder structure
- Developing user guidelines and procedures, finding/mapping aids, and delivering training (formal or desk-side) to staff on the use and maintenance of the new shared drive folder structure

#### Reporting Requirements

- Providing briefings, status updates/reports, and final results reports as requested
- Maintaining statistics/metrics for project tracking and communication purposes
- Maintaining a current work plan and project schedule

### TERMS

The term of this Agreement commences on April 19, 2021 and ends on March 31, 2022.

### KEY PERSONNEL

All notice to the Commission will be sent to the Contract Manager:

**Kathryn Smerechinskiy**  
2950 Jutland Road  
Victoria, BC V8T 5K2  
250-419-4487

The Key Personnel of the Contractor are as follows:

- (a) Marion Villines

Contractor Initials: \_\_\_\_\_

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE B Fees and Expenses

This Schedule forms part of the agreement

Contract No: 25122001

1. Fees will be paid at an hourly/daily rate of: \$55 per hour/day (8 hrs = 1 day), for the term during which the Contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, and in no event will the fees payable to the Contractor in accordance with this paragraph exceed, in aggregate, \$75,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).
2. The Contractor should submit to the Commission, upon completion of the project, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.
3. After receipt by the Commission of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.
4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is \$75,000 plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: SP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



**SCHEDULE C**  
**Approved Sub-contractor**

This Schedule forms part of the agreement

Contract No: 25122001

The following sub-contractor(s) has been approved under this Agreement:

1. Marion Villines

Contractor Initials: MP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE D Insurance

This Schedule forms part of the agreement

Contract No: 25122001

### Insurance:

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Commission:
  - (a) Commercial General Liability in an amount not less than **\$2,000,000.00** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
    - (i) include the Commission as an additional insured,
    - (ii) be endorsed to provide the Commission with 30 days advance written notice of cancellation or material change, and
    - (iii) include a cross liability clause.
2. All insurance described in section 1 of this Schedule must:
  - (a) be primary; and
  - (b) not require the sharing of any loss by any insurer of the Commission.
3. The Contractor must provide the Commission with evidence of all required insurance as follows:
  - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Commission evidence of all required insurance in the form of a completed Certificate of Insurance;
  - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Commission within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Province of British Columbia Certificate of Insurance; and
  - (c) despite paragraph (a) or (b) above, if requested by the Commission at any time, the Contractor must provide to the Commission certified copies of the required insurance policies.
4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: AP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE E Privacy Protection

This Schedule forms part of the agreement.

Contract No: 25122001

### Definitions

1. In this Schedule,
  - (a) "Act" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
  - (b) "contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
  - (c) "personal information" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Commission and the Contractor dealing with the same subject matter as the Agreement.

### Purpose

2. The purpose of this Schedule is to:
  - (a) enable the Commission to comply with its statutory obligations under the Act with respect to personal information; and
  - (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

### Collection of personal information

3. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
  - (a) the purpose for collecting it;
  - (b) the legal authority for collecting it; and
  - (c) the title, business address and business telephone number of the person designated by the Commission to answer questions about the Contractor's collection of personal information.

### Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Commission to make a decision that directly affects the individual the information is about.

### Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission unless the Agreement expressly requires the Contractor to provide such access and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

### Correction of personal information

8. Within 5 business days of receiving a written direction from the Commission to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
9. When issuing a written direction under section 8, the Commission must advise the Contractor of the date the correction request to which the direction relates was received by the Commission in order that the Contractor may comply with section 10.
10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Commission, the Contractor disclosed the information being corrected or annotated.
11. If the Contractor receives a request for correction of personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

### Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

### Storage and access to personal information

13. Unless the Commission otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Contractor Initials: LP

Oil and Gas Commission (authorized initials) \_\_\_\_\_



## SCHEDULE E Privacy Protection

This Schedule forms part of the agreement.

Contract No: 25122001

### Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Commission in writing to dispose of it or deliver it as specified in the direction.

### Use of personal information

15. Unless the Commission otherwise directs in writing, the Contractor may only use personal information if that use is:
- (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
  - (b) in accordance with section 13.

### Disclosure of personal information

16. Unless the Commission otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Commission if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
17. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

### Inspection of personal information

18. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

### Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
- (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
  - (b) any direction given by the Commission under this Schedule.
20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

### Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Commission of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

### Termination of Agreement

22. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

### Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
26. If a provision of the Agreement (including any direction given by the Commission under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

### Definitions

Contractor Initials: SP

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE G Security

This Schedule forms part of the agreement.

Contract No: 25122001

1. In this Schedule,
  - a. "Equipment" means any equipment, including interconnected systems or subsystems of equipment, software and networks, used or to be used by the Contractor to provide the Services;
  - b. "Facilities" means any facilities at which the Contractor provides or is to provide the Services;
  - c. "Information" means information
    - i. in the Material, or
    - ii. accessed, produced or obtained by the Contractor (whether verbally, electronically or otherwise) as a result of the Agreement;
  - d. "Record" means a "record" as defined in the Interpretation Act;
  - e. "Sensitive Information" means
    - i. Information that is "personal information" as defined in the Freedom of Information and Protection of Privacy Act, or
    - ii. any other Information specified as "Sensitive Information" in Appendix G6, if attached; and
  - f. "Services Worker" means an individual involved in providing the Services for or on behalf of the Contractor and, for greater certainty, may include
    - i. the Contractor or a subcontractor if an individual, or
    - ii. an employee or volunteer of the Contractor or of a subcontractor.

### Schedule contains additional obligations

2. The obligations of the Contractor in this Schedule are in addition to any other obligations in the Agreement or the schedules attached to it relating to security including, without limitation, the obligations of the Contractor in the Privacy Protection Schedule, if attached.

### Services Worker confidentiality agreements

3. The Contractor must not permit a Services Worker who is an employee or volunteer of the Contractor to have access to Sensitive Information unless the Services Worker has first entered into a confidentiality agreement with the Contractor to keep Sensitive Information confidential on substantially similar terms as those that apply to the Contractor under the Agreement.

### Services Worker security screening

4. The Contractor may only permit a Services Worker who is an employee or a volunteer of the Contractor to have access to Sensitive Information or otherwise be involved in providing the Services if, after having subjected the Services Worker to the personnel security screening requirements and any additional requirements the Contractor may consider appropriate, the Contractor is satisfied that the Services Worker does not constitute an unreasonable security risk.

Contractor Initials: 

Oil and Gas Commission (authorized initials): \_\_\_\_\_





## SCHEDULE G Security

This Schedule forms part of the agreement.

Contract No: 25122001

### Services Worker activity logging

5. Subject to section 6, the Contractor must create and maintain detailed Records logging the activities of all Service Workers in relation to:
  - a. their access to Sensitive Information; and
  - b. other matters specified by the Commission in writing for the purposes of this section.
6. The Records described in section 5 must be made and maintained in a manner, and contain information, specified in Appendix G2, if attached.

### Facilities and Equipment protection and access control

7. The Contractor must create, maintain and follow a documented process to:
  - a. protect Facilities and Equipment of the Contractor required by the Contractor to provide the Services from loss, damage or any other occurrence that may result in any of those Facilities and Equipment being unavailable when required to provide the Services; and
  - b. limit access to Facilities and Equipment of the Contractor
    - i. being used by the Contractor to provide the Services, or
    - ii. that may be used by someone to access Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons.
8. If the Commission makes available to the Contractor any Facilities or Equipment of the Commission for the use of the Contractor in providing the Services, the Contractor must comply with any policies and procedures provided to it by the Commission on acceptable use, protection of, and access to, such Facilities or Equipment.

### Sensitive Information access control

9. The Contractor must:
  - a. create, maintain and follow a documented process for limiting access to Sensitive Information to those persons who are authorized to have that access and for the purposes for which they are authorized, which process must include measures to verify the identity of those persons; and
  - b. comply with the information access control requirements set out in Appendix G3, if attached.

### Integrity of Information

10. The Contractor must:
  - a. create, maintain and follow a documented process for maintaining the integrity of Information while possessed or accessed by the Contractor; and
  - b. comply with the information integrity requirements set out in Appendix G4, if attached.
11. For the purposes of section 10, maintaining the integrity of Information means that, except to the extent expressly authorized by the Agreement or approved in writing by the Commission, the Information has:
  - a. remained as complete as when it was acquired or accessed by the Contractor; and
  - b. not been altered in any material respect.

Contractor Initials:                     

Oil and Gas Commission (authorized initials):



## SCHEDULE G Security

This Schedule forms part of the agreement.

Contract No: 25122001

### Documentation of changes to processes

12. The Contractor must create and maintain detailed Records logging any changes it makes to the processes described in sections 7, 9 and 10.

### Notice of security breaches

13. If Contractor becomes aware that:
  - a. unauthorized access, collection, use, disclosure, alteration or disposal of Information or Records containing Information; or
  - b. unauthorized access to Facilities or Equipment has occurred or is likely to occur (whether or not related to a failure by the Contractor to comply with this Schedule or the Agreement), the Contractor must immediately notify the Commission of the particulars of that occurrence or likely occurrence. If the Contractor provides a notification under this section other than in writing, that notification must be confirmed in writing to the Commission as soon as it is reasonably practicable for the Contractor to do so.

### Review of security breaches

14. If the Commission decides to conduct a review of a matter described in section 13 (whether or not the matter came to the attention of the Commission as a result of a notification under section 13), the Contractor must, on the request of the Commission, participate in the review to the extent that it is reasonably practicable for the Contractor to do so.

### Retention of Records

15. Unless the Agreement otherwise specifies, the Contractor must retain all Records in the Contractor's possession that contain Information until directed by the Commission in writing to dispose of them or deliver them as specified in the direction.

### Storage of Records

16. Until disposed of or delivered in accordance with section 15, the Contractor must store any Records in the Contractor's possession that contain Information in accordance with the provisions of Appendix G5, if attached.

### Audit

17. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy:
  - a. any Records in the possession of the Contractor containing Information; or
  - b. any of the Contractor's Information management policies or processes (including the processes described in sections 7, 9 and 10 and the logs described in sections 5 and 12) relevant to the Contractor's compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to the exercise by the Commission of the Commission's rights under this section.

Contractor Initials: \_\_\_\_\_

Oil and Gas Commission (authorized initials): \_\_\_\_\_



## SCHEDULE G Security

This Schedule forms part of the agreement.

Contract No: 25122001

### Termination of Agreement

18. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

### Interpretation

19. In this Schedule, unless otherwise specified:
- references to sections are to sections of this Schedule; and
  - references to appendices are to the appendices attached to this Schedule.
20. Any reference to the "Contractor" in this Schedule includes any subcontractor retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors comply with this Schedule.
21. The appendices attached to this Schedule are part of this Schedule.
22. If there is a conflict between a provision in an appendix attached to this Schedule and any other provision of this Schedule, the provision in the appendix is inoperative to the extent of the conflict unless the appendix states that it operates despite a conflicting provision of this Schedule.
23. If there is a conflict between:
- a provision of the Agreement, this Schedule or an appendix attached to this Schedule; and
  - a documented process required by this Schedule to be created or maintained by the Contractor
- the provision of the Agreement, Schedule or appendix will prevail to the extent of the conflict.
24. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.

Contractor Initials:     *AP*    

Oil and Gas Commission (authorized initials): \_\_\_\_\_



CONTRACT No. 25122001

**CONTRACT AMENDMENT #2**

THIS AMENDMENT MADE THIS 25<sup>th</sup> DAY OF MARCH 2022

**BETWEEN:**

**OIL AND GAS COMMISSION (HEREIN CALLED THE "COMMISSION")  
OF THE FIRST PART**

**AND:**

**FILE IT SOLUTIONS (HEREIN CALLED THE "CONTRACTOR")  
OF THE SECOND PART**

**WITNESSETH THAT WHEREAS:**

- A. The parties hereto entered into a General Services Agreement identified as Contract No. **25122001** (the "Agreement") for a term which initially commenced on April 19, 2021 and was scheduled to end on March 31, 2022;
- B. **AND WHEREAS** the parties have agreed to modify the Agreement.

**NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:**

- 1. This amendment and renewal of the Agreement is made effective April 1, 2022.
- 2. The term of the contract is to be extended to March 2023. The term described in Schedule "A" is deleted and replaced with:  
  
The term of this Agreement commences on April 19, 2021 and is scheduled to end on March 31, 2023. The Commission has discretion to offer a one-year renewal of services at that time.
- 3. Maximum fees will increase by \$75,000 from \$75,000 to \$150,000. Schedule B, Clauses 1 and 4 will be deleted and replace with:  
  
1. Fees will be paid at an hourly rate of: \$55 per hour for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract and in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, \$150,000, exclusive of any applicable taxes.  
  
6. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is **\$150,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.
- 4. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

**IN WITNESS WHEREOF** the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the <u>29</u> day of March 2022 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the <u>25</u> day of March 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
<i>K. Smerechinskiy</i>	<i>Laurie Phillips</i>
Signature	Signature
<b>Kathryn Smerechinskiy</b>	<b>Laurie Phillips</b>
Print Name	Print Name



# Information Technology Professional Service Agreement

For Administration Purpose Only

Account No: 15000-214-000005

Solicitation No: RFP21422003

Contract No: 21422002

BETWEEN	AND
<b>Oil and Gas Commission</b> also referred to as the "Commission"	<b>Gravity Union Solutions Limited</b> also referred to as the "Contractor"
(the "Commission", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	1240 - 605 Robson Street Vancouver, BC V6B 5J3
Phone number: 250.419.4400	Phone Number: 604.782.1507
Email: <a href="mailto:procurement@bcogc.ca">procurement@bcogc.ca</a>	Email: <a href="mailto:mschweitzer@gravityunion.com">mschweitzer@gravityunion.com</a>

THE OIL AND GAS COMMISSION AND THE CONTRACTOR AGREE TO THE TERMS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.

**SCHEDULE A – list of Services:** Development Services – Modern Digital Workplace (See attached)

**Term: Start Date:** February 1, 2022

**End Date:** March 31, 2024

<b>SCHEDULE B - FEES AND EXPENSES:</b>	
Fees: \$ 200,000	Expenses: \$
Billing Date(s): <b>Monthly / Upon Invoice</b>	Maximum Amount: <b>\$ 200,000</b>



**SCHEDULE C - APPROVED SUBCONTRACTOR(S):**  
N/A

**SCHEDULE D - INSURANCE:**  
(See Attached)

**SCHEDULE E – PRIVACY PROTECTION:**  
(See Attached)

**SCHEDULE F – ADDITIONAL TERMS:**  
N/A

**SCHEDULE G – SECURITY:**  
N/A

SIGNED AND DELIVERED on the <u>14</u> <sup>th</sup> day of February 2022 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the <u>14</u> day of February 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
<b>Ab Dosil</b>	<b>Michael Schweitzer</b>
Print Name	Print Name

**READ TERMS ON THE FOLLOWING PAGES**

**TERMS OF INFORMATION TECHNOLOGY  
PROFESSIONAL SERVICE AGREEMENT**

**1 DEFINITIONS**

**General**

- 1.1 In this Agreement, unless the context otherwise requires:
- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
  - (b) "Incorporated Material" means any material in existence prior to the start of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
  - (c) "Material" means the Produced Material and the Received Material;
  - (d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced or provided by the Contractor or a Subcontractor and includes the Incorporated Material;
  - (e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Commission or any other person;
  - (f) "Services" means the services described in Part 2 of Schedule A;
  - (g) "Subcontractor" means a person described in paragraph (a) or (b) of section 13.4; and
  - (h) "Term" means the term of the Agreement described in Part 1 of Schedule A subject to that term ending earlier in accordance with this Agreement.

**Meaning of "record"**

- 1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

**2 SERVICES**

**Provision of services**

- 2.1 The Contractor must provide the Services in accordance with this Agreement.

**Term**

- 2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

**Supply of various items**

- 2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

**Standard of care**

- 2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill, and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

**Standards in relation to persons performing Services**

- 2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

**Instructions by Commission**

- 2.6 The Commission may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions, but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are carried out.

**Confirmation of non-written instructions**

- 2.7 If the Commission provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Commission in writing, which request the Commission must comply with as soon as it is reasonably practicable to do so.

**Effectiveness of non-written instructions**

- 2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

**Applicable laws**

- 2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

**3 PAYMENT**

**Fees and expenses**

- 3.1 If the Contractor complies with this Agreement, then the Commission must pay to the Contractor at the times and on the conditions set out in Schedule B:
- (a) the fees described in that Schedule;
  - (b) the expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Commission's opinion, are necessarily incurred by the Contractor in providing the Services; and
  - (c) any applicable taxes payable by the Commission under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Commission is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

**Statements of accounts**

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Commission a written statement of account in a form satisfactory to the Commission upon completion of the Services or at other times described in Schedule B.

**Withholding of amounts**

- 3.3 Without limiting section 9.1, the Commission may withhold from any payment due to the Contractor an amount sufficient to indemnify in whole or in part the Commission and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Commission to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Commission.

**Appropriation**

- 3.4 The Commission's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Commission during which payment becomes due.

**Currency**

- 3.5 Unless otherwise specified in this Agreement, all references to money are to Canadian dollars.

**Non-resident income tax**

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Commission may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

**Prohibition against committing money**

- 3.7 Without limiting section 13.10(a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Commission to pay any money except as may be expressly provided for in this Agreement.

**Refunds of taxes**

- 3.8 The Contractor must:
- (a) apply for, and use reasonable efforts to obtain, any available refund, credit, rebate or remission of federal, provincial or other tax or duty imposed on the Contractor as a result of this Agreement that the Commission has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement; and
  - (b) immediately on receiving, or being credited with, any amount applied for under paragraph (a), remit that amount to the Commission.

**4 REPRESENTATIONS AND WARRANTIES**

- 4.1 As at the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Commission as follows:
- (a) except to the extent the Contractor has previously disclosed otherwise in writing to the Commission,
    - (i) all information, statements, documents and reports furnished or submitted by the Contractor to the Commission in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct;
    - (ii) the Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractual or other agreements in place and available to enable the Contractor to fully perform the Services and to grant any licenses under this Agreement; and
    - (iii) the Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and

Contractor Initials:

*MS*

Oil and Gas Commission (authorized initials):

**TERMS OF INFORMATION TECHNOLOGY  
PROFESSIONAL SERVICE AGREEMENT**

- (b) if the Contractor is not an individual,
- (i) the Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and this Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.
  - (ii) the Contractor is not an individual,

**5 PRIVACY, SECURITY AND CONFIDENTIALITY**

**Privacy**

- 5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

**Security**

- 5.2 The Contractor must:
- (a) make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, alteration or disposal; and

**Confidentiality**

- 5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Commission's prior written consent except:
- (a) as required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
  - (b) if it is information that is generally known to the public other than as result of a breach of this Agreement; or
  - (c) if it is information in any Incorporated Material.

**Public announcements**

- 5.4 Any public announcement relating to this Agreement will be arranged by the Commission and, if such consultation is reasonably practicable, after consultation with the Contractor.

**Restrictions on promotion**

- 5.5 The Contractor, must not, without the prior written approval of the Commission, refer for promotional purposes to the Commission being a customer of the Contractor or the Commission having entered into this Agreement.

**6 MATERIAL AND INTELLECTUAL PROPERTY**

**Access to Material**

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Commission, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Commission.

**Ownership and delivery of Material**

- 6.2 The Commission exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Commission immediately upon the Commission's request.

**Matters respecting intellectual property**

- 6.3 The Commission exclusively owns all intellectual property rights, including copyright, in:
- (a) Received Material that the Contractor receives from the Commission; and
  - (b) Produced Material, other than any Incorporated Material.

Upon the Commission's request, the Contractor must deliver to the Commission documents satisfactory to the Commission that irrevocably waive in the Commission's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Commission of the copyright in the Produced Material, other than any Incorporated Material.

**Rights in relation to Incorporated Material**

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Commission:
- (a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to exercise, in respect of that Incorporated Material, the rights set out in the *Copyright Act* (Canada), including the right to use, reproduce, modify, publish and distribute that Incorporated Material; and
  - (b) the right to sublicense or assign to third-parties any or all of the rights granted to the Commission under section 6.4(a).

**Right of Commission to negotiate license of Produced Material**

- 6.5 After the end of the Term, the Commission in its sole discretion, may negotiate with the Contractor to provide the Contractor a license (which may be exclusive or non-exclusive) for the Contractor to use, reproduce, modify or distribute some or all of the Produced Material.

**7 RECORDS AND REPORTS**

**Work reporting**

- 7.1 Upon the Commission's request, the Contractor must fully inform the Commission of all work done by the Contractor or a Subcontractor in connection with providing the Services.

**Time and expense records**

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Commission. Unless otherwise specified in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement ends.

**8 AUDIT**

- 8.1 In addition to any other rights of inspection the Commission may have under statute or otherwise, the Commission may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Commission's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Commission of the Commission's rights under this section.

**9 INDEMNITY AND INSURANCE**

**Indemnity**

- 9.1 The Contractor must indemnify and save harmless the Commission and the Commission's employees and agents from any loss, claim (including any claim of infringement of third-party intellectual property rights), damage award, action, cause of action, cost or expense that the Commission or any of the Commission's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, (each a "Loss") to the extent the Loss is directly or indirectly caused or contributed to by:
- (a) any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement; or
  - (b) any representation or warranty of the Contractor being or becoming untrue or incorrect.

**Monetary limitations of indemnity**

- 9.2 The indemnification by the Contractor pursuant to section 9.1 is limited to:
- (a) \$2,000,000 per Loss; and
  - (b) \$4,000,000 in the aggregate for all Losses.

**Exceptions to monetary limitations**

- 9.3 The limitations set out in section 9.2 do not apply to a Loss resulting from or relating to any of the following:
- (a) bodily injury or damage to real property or tangible personal property;
  - (b) third-party intellectual property rights; or
  - (c) a breach of section 5.1, 5.2, 5.3 or 6.1 of this Agreement.

**Commission to notify Contractor of Loss**

- 9.4 To claim indemnification for a Loss pursuant to section 9.1, the Commission must notify the Contractor in writing of the Loss as soon as reasonably practicable after the Commission becomes aware of the Loss provided that a failure by the Commission to provide such notification will not invalidate the claim unless the Contractor is materially prejudiced by that failure.

**Third-party intellectual property infringement claims**

- 9.5 If the Loss is on the basis of a third-party claim that any element of the Material infringes the intellectual property rights of any person,
- (a) then, without limiting section 9.1, the Contractor must defend the Commission against that claim at the Contractor's expense and the Contractor must pay all associated costs, damages and legal fees that a court or arbitrator finally awards or are included in a settlement agreed to by the Contractor; and
  - (b) the Commission must cooperate with the Contractor in the defence of the claim and, where appropriate in the discretion of the Commission, will allow the Contractor to appoint and instruct counsel and otherwise control the defence and any related settlement negotiations.

**Insurance**

- 9.6 The Contractor must comply with the Insurance Schedule attached as Schedule D.

**Workers compensation**

- 9.7 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): [Signature]

**TERMS OF INFORMATION TECHNOLOGY  
PROFESSIONAL SERVICE AGREEMENT**

**Personal optional protection**

- 9.8 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
- (a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
  - (b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

**Evidence of coverage**

- 9.9 Within 10 Business Days of being requested to do so by the Commission, the Contractor must provide the Commission with evidence of the Contractor's compliance with sections 9.7 and 9.8.

**10 FORCE MAJEURE**

**Definitions relating to force majeure**

- 10.1 In this section and sections 10.2 and 10.3:
- (a) "Event of Force Majeure" means one of the following events:
    - (i) a natural disaster, fire, flood, storm, epidemic or power failure,
    - (ii) a war (declared and undeclared), insurrection or act of terrorism or piracy,
    - (iii) a strike (including illegal work stoppage or slowdown) or lockout, or
    - (iv) a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
  - (b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

**Consequence of Event of Force Majeure**

- 10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

**Duties of Affected Party**

- 10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

**11 DEFAULT AND TERMINATION**

**Definitions relating to default and termination**

- 11.1 In this section and sections 11.2 to 11.4:
- (a) "Event of Default" means any of the following:
    - (i) an Insolvency Event,
    - (ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
    - (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and
  - (b) "Insolvency Event" means any of the following:
    - (i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up,
    - (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency,
    - (iii) a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor,
    - (iv) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada),
    - (v) a receiver or receiver-manager is appointed for any of the Contractor's property, or
    - (vi) the Contractor ceases, in the Commission's reasonable opinion, to carry on business as a going concern.

**Commission's options on default**

- 11.2 On the happening of an Event of Default, or at any time thereafter, the Commission may, at its option, elect to do any one or more of the following:
- (a) by written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
  - (b) pursue any remedy or take any other action available to it at law or in equity; or
  - (c) by written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

**Delay not a waiver**

- 11.3 No failure or delay on the part of the Commission to exercise its rights in relation to an Event of Default will constitute a waiver by the Commission of such rights.

**Commission's right to terminate other than for default**

- 11.4 In addition to the Commission's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Commission may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

**Payment consequences of termination**

- 11.5 Unless Schedule B otherwise provides, if the Commission terminates this Agreement under section 11.4:
- (a) the Commission must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Commission's satisfaction before termination of this Agreement; and
  - (b) the Contractor must, within 30 days of such termination, repay to the Commission any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Commission has notified the Contractor in writing was not completed to the Commission's satisfaction before termination of this Agreement.

**Discharge of liability**

- 11.6 The payment by the Commission of the amount described in section 11.5(a) discharges the Commission from all liability to make payments to the Contractor under this Agreement.

**Notice in relation to Events of Default**

- 11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Commission of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

**12 DISPUTE RESOLUTION**

**Dispute resolution process**

- 12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
- (a) the parties must initially attempt to resolve the dispute through collaborative negotiation;
  - (b) if the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the Mediate BC Society; and
  - (c) if the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Arbitration Act*.

**Location of arbitration or mediation**

- 12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

**Costs of arbitration or mediation**

- 12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a arbitration or mediation under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

**13 MISCELLANEOUS**

**Delivery of notices**

- 13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
- (a) by email to the addressee's email specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
  - (b) by hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
  - (c) by prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

**Change of address or email**

- 13.2 Either party may from time to time give notice to the other party of a substitute address or email, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email specified for the party giving the notice.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): 



**TERMS OF INFORMATION TECHNOLOGY  
PROFESSIONAL SERVICE AGREEMENT**

**Assignment**

13.3 The Contractor must not assign any of the Contractor's rights or obligations under this Agreement without the Commission's prior written consent. Upon providing written notice to the Contractor, the Commission may assign to any person any of the Commission's rights under this Agreement and may assign to any "government corporation", as defined in the *Financial Administration Act*, any of the Commission's obligations under this Agreement

**Subcontracting**

13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Commission's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:

- (a) any person retained by the Contractor to perform obligations under this Agreement; and
- (b) any person retained by a person described in paragraph (a) to perform those obligations fully complies with this Agreement in performing the subcontracted obligations.

**Waiver**

13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

**Modifications**

13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

**Entire agreement**

13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to performance of the Services.

**Survival of certain provisions**

13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.5, 7.1, 7.2, 8.1, 9.1 to 9.6, 9.9, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

**Schedules**

13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

**Independent contractor**

13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:

- (a) an employee or partner of the Commission; or
- (b) an agent of the Commission except as may be expressly provided for in this Agreement.

The Contractor must not act or purport to act contrary to this section.

**Personnel not to be employees of Commission**

13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Commission.

**Key Personnel**

13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in Part 4 of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Commission otherwise approves in writing, which approval must not be unreasonably withheld.

**Pertinent information**

13.13 The Commission must make available to the Contractor all information in the Commission's possession which the Commission considers pertinent to the performance of the Services.

**Conflict of interest**

13.14 The Contractor must not provide any services to any person in circumstances which, in the Commission's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Commission under this Agreement.

**Time**

13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

**Conflicts among provisions**

13.16 Conflicts among provisions of this Agreement will be resolved as follows:

- (a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
- (b) a provision in a schedule will prevail over any conflicting provision in a document attached to, or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

**Agreement not permit nor fetter**

13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Commission or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Commission or its agencies of any statutory, prerogative, executive or legislative power or duty.

**Remainder not affected by invalidity**

13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

**Further assurances**

13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

**Additional terms**

13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

**Governing law**

13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

**14 INTERPRETATION**

14.1 In this Agreement:

- (a) "includes" and "including" are not intended to be limiting;
- (b) unless the context otherwise requires, references to sections by number are to sections of this Agreement;
- (c) the Contractor and the Commission are referred to as "the parties" and each of them as a "party";
- (d) "attached" means attached to this Agreement when used in relation to a schedule;
- (e) unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
- (f) the headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
- (g) "person" includes an individual, partnership, corporation or legal entity of any nature; and
- (h) unless the context otherwise requires, words expressed in the singular include the plural and vice versa.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): AD

This Schedule forms part of the agreement.

Contract No: 21422002

### Description of Services

The Contractor will provide services as proposed in December 2021 and as described below to architect and develop a high availability, collaborative and integrated digital workplace built on the M365 platform.

Services will include, but are not limited to the following as described in the original request:

- Project management services using industry best practices for iterative delivery
- Implementation of necessary M365 (and other integrated) services to deliver the scope, including
  - o Technical analysis
  - o UX and Design proposal
  - o Development and implementation of sites and integrations
  - o Testing and training technical staff
  - o Migration to production
  - o Ongoing go-live support
- Expert resources capable of ensuring the project meets objectives through effective and sustainable adoption of new tools
  - o Stakeholder engagement and analysis
  - o User experience considerations when designing services
  - o Provide user training
  - o Change management services to help effective adoption
  - o Collaboration with Commission staff to transition to operations
  - o Set up governance and document best practices
  - o Security and privacy consultation when developing components of the digital workplace

The Commission will provide the following:

- Collaboration to ensure the project is aligned with intended objectives
- Business and technical product owners of various components of the digital workplace
- Access to business and technical SMEs, stakeholders, and sponsor
- Licensing and necessary access to Commission's M365 tenant
- Project champions to help mediate issues and resolve blockers

### Outcomes

This initiative will be deemed successful when the following outcomes are realized. Based on staff interviews conducted during M365 evaluation, and in alignment with the Commission's Digital Workplace Program, this initiative aims to accomplish the following outcomes:

- Implement workplace tools that are user friendly and intuitive
- Ensure information is easily searchable and securely shareable
- Collaborate in real time, and remotely, in a digital environment
- Effectively manage asynchronous communication
- Socialize with other staff in a virtual environment using modern platforms
- Support communication and information access on the go securely (e.g., on mobile devices)
- Provide department ownership and control over their content
- Provide user process centric training to ensure effective adoption across staff with varied learning methods and demographics
- Ensure document libraries and migration of documents are aligned with the Commission's Electronic Document Retention and Management (EDRM) plan and recommendations
- Ensure a smooth process for complying with records management policies (e.g., applying document tags and retention policies)
- Apply governance structures that provide effective oversight to ensure a sustainable workplace implementation

Contractor Initials: MS

Oil and Gas Commission (authorized initials): AD

This Schedule forms part of the agreement.

Contract No: 21422002

**Outcomes (Cont.)**

- Supply a sustainable and scalable digital workplace architecture and processes to ensure effective ongoing operations
- Guarantee all services comply with the Freedom of Information and Protection of Privacy Act (FOIPPA), IT Infrastructure best practices, Commission's cybersecurity, and record management policies

The Commission expects the following to be part of the implementation:

- Technical and Logical SharePoint structure
  - o The Commission is leaning towards a flat technical structure (i.e. not using subsites) to ensure ongoing flexibility
  - o Sites can include employee facing sites (i.e. corporate), department sites (focused on individual departments), and project sites (focused on cross department teams)
- The logical structure (navigation, hierarchy, etc.) will be developed in parallel using the Navigation Mega Menu.
- Site Templates
  - o Develop corporate branding across all pages
    - Common navigation
    - Common theme / colours
    - Unified search
    - Roll-up of News and Events
  - o Develop standardized templates for (but not limited to)
    - Landing pages (department welcome pages, employee areas, etc.)
    - Logical subsites (e.g., department public and private pages, project pages)
    - Newsletters
    - News articles
- Multimedia management
  - o Implement any multimedia file management tools (such as Streams) to enable easy and secure sharing of multimedia files, such as videos, images
- Document management and migration
  - o Assist in migrating documents from shared drives and web servers to OneDrive or SharePoint
  - o Assist in converting documents to site pages, where appropriate
  - o Ensure records management policies are applied during migration
- Sustainable metadata usage
  - o Work with the governance team to set up content within the term store
  - o Ensure services implemented (e.g., document libraries) utilize meta data from the term store
  - o Help develop policies for meta data usage and incorporate them into the centre of excellence
- Implement search refiners to ensure efficient and relevant content searching
- Collaboration
  - o Review and refine the current Teams implementation to ensure effective use of Teams for collaboration and integration into other M365 services
- Socialization Platform
  - o Implement a social media platform, such as Yammer, to enable non-business-related conversations
  - o Assist in developing governance policies to ensure the platform follows Commission guidelines
- Sharing Corporate Information such as
  - o News and Exec Updates
  - o Internal staff updates (corporate and department level)
  - o Newsletters (corporate and department level)
  - o Appropriate combination of tools to publish and share content
- Adoption
  - o User/Process centric training materials and adoption plan
  - o Identify and develop training materials (including but not limited to recorded training sessions, manuals, short videos, new staff handbook, etc.)

Contractor Initials:

*MS*

Oil and Gas Commission (authorized initials):



This Schedule forms part of the agreement.

Contract No: 21422002

- Provide training to staff and other Commission trainers
- Create a detailed plan and execute on change management activities
- Governance and Centre of Excellence
  - Help establish a sustainable centre of excellence and governance structure
  - Help establish a documentation hub for centre of excellence
  - Develop guidelines and best practices to sustainably maintain the centre of excellence
- Security
  - Defined security roles from M365 Global Administrators to End Users
  - A simple three-group security model for sites
    - Site Owners – Full Control
    - Site Members – Edit
    - Site Visitors – Read
  - Company-wide security groups
  - No external sharing of Commission information or data with the possible exception of project sites

The successful proponent is not expected to implement or re-implement:

- Any M365 services the Commission has already implemented, such as Teams
- Any setup of specific records management labels, classification, or policies

### Reporting Requirements

Weekly a detailed status report will be delivered to BC Oil and Gas Commission's Project Manager. This report will contain at least the following information:

- Activities completed and progress against work plan(s) for the current week
- Issues requiring immediate attention by key personnel or impending deadlines for the project team's responsibilities (including projected impacts if deadlines are missed)
- Activities planned for the following week
- Running log of issues and risks
- Management of approvals and signoffs
- Financial summary

1. The Contractor agrees and confirms as follows:

- a. All Contractor representatives, employees, sub-contractor representatives or sub-contractor employees attending a Commission office or field-based worksite at any time on or after January 10, 2022 will:
  - i. be fully vaccinated against COVID-19 with a vaccine approved in Canada, including any available recommended booster doses; or
  - ii. have received an exemption from the requirement to be fully vaccinated against COVID-19 from the Office of the Provincial Health Officer or for a valid reason under the BC Human Rights Code.
- b. All Contractor representatives, employees, sub-contractor representatives or sub-contractor employees providing services relating to this Agreement will be provided with notice of the vaccination requirements identified in 1(a) prior to attending a Commission office or field-based worksite on or after January 10, 2022 and will be required to maintain proof of valid vaccination status.
- c. The Contractor will obtain from each sub-contractor a true, accurate written certification of the sub-contractor's compliance with these vaccination requirements.
- d. The Contractor agrees to provide the Commission with a true, accurate written certification of compliance with 1(a)-(c) at any time and agrees that such certification may be subject to verification by the Commission at any time.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): [Signature]



# SCHEDULE A SERVICES

This Schedule forms part of the agreement.

Contract No: 21422002

## TERM

The term of this Agreement commences on February 1, 2022 and ends on March 31, 2024.

Work will be completed in 2 stages

Stage 1: Complete the scope of work including Digital Workplace foundations, implementation of the corporate portal, board portal, and initial department sites as prioritized with a total value up to \$200,000.

Stage 2: On completion of stage one, an assessment will be completed to determine options for implementing stage two. Stage 2 will focus on additional Department, Team, and Project sites and may include overall improvements to the Digital Workplace implementation. Stage 2 will have a maximum value of \$296,000 with work likely to begin in FY2023/24. This is subject to budget approval and the results and value realized from stage one of the project.

This is summarized in the following table

Stage	Phase	% Budget	Hours	Cost
1.	1. Foundation	12.5%	320	\$61,950
	2. Corporate Portal	12.5%	320	\$61,950
	3. Board Portal	6.25%	160	\$30,975
	4. Initial Department Sites	8.75%	224	\$45,125
	Sub Total	40%	1024	\$200,000
2.	5. Departmental, Teams and Projects (160 hours per site) <sup>1</sup>	60%	1536	\$296,600
	Total	100%	2560	\$496,600

## KEY PERSONNEL

All notices to the Commission will be sent to the Contract Manager:

Abhinav Rai  
Manager, Business Intelligence, Research & Analytics  
[abhinav.rai@bcogc.ca](mailto:abhinav.rai@bcogc.ca)

Derek Mathews  
Director, Architecture & Innovation  
[derek.mathews@bcogc.ca](mailto:derek.mathews@bcogc.ca)

Invoices will be sent to:

Abhinav Rai  
Manager, Business Intelligence, Research & Analytics  
[abhinav.rai@bcogc.ca](mailto:abhinav.rai@bcogc.ca)

<sup>1</sup> Stage 2 above is dependent on the number of business units the Commission chooses to onboard into the new Digital Workplace portal.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): [Signature]

This Schedule forms part of the agreement.

Contract No: 21422002

Derek Mathews  
**Director, Architecture & Innovation**  
[derek.mathews@bcogc.ca](mailto:derek.mathews@bcogc.ca)

Lisa Gerlach  
**Manager, Communications**  
[lisa.gerlach@bcogc.ca](mailto:lisa.gerlach@bcogc.ca)

Katie Cook  
**Information Systems & Technology Project Coordinator • Planning & Technology**  
[katie.cook@bcogc.ca](mailto:katie.cook@bcogc.ca)

The Key Personnel of the Contractor are as follows:

- a. Michael Schweitzer | Vancouver, BC – CEO, Founder, and Lead Consultant
- b. Kyal Creswell | Ottawa, Ont. – Solution Architect
- c. Ellisa Kilmos | Vancouver, BC – Senior Consultant/UX Lead
- d. Pauline Richer | Calgary, AB – M365 Consultant
- e. Kelvin Yu | Vancouver, BC – M365 Consultant
- f. Matt James | Calgary, AB – Senior Project Manager
- g. Laura Bower | Vancouver, BC – Project Coordinator

Contractor Initials: MS

Oil and Gas Commission (authorized initials): AD

## SCHEDULE B Fees and Expenses

This Schedule forms part of the agreement.

Contract No: 21422002

1. Fees will be paid at an hourly rate as estimated and outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, \$200,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Phase	% Budget	Hours	Cost
<b>1 – Foundation</b>	12.5%	320	\$61,950
<b>2 – Corporate and M365 Baseline Setup</b>	12.5%	320	\$61,950
<b>3 – Departmental, Teams and Project Sites (12 department sites @ 160 hours per department site)</b>	75%	1,920	\$371,700
<b>Total</b>	100.0%	2,560	\$496,600

### Estimate By Role

Role	% Budget	Hours	Cost
<b>Senior Project Manager</b>	10.6%	271	\$54,200
<b>Lead Consultant</b>	7%	180	\$45,000
<b>Senior Solution Architect</b>	10.5%	270	\$67,500
<b>Senior Infrastructure Architect</b>	11.1%	283	\$56,600
<b>Digital Transformation Analyst 1</b>	30.4%	778	\$136,150
<b>Digital Transformation Analyst 2</b>	30.4%	778	\$136,150
<b>Total</b>	100.0%	2,560	\$496,600

Role	Rate (per hour)
<b>Senior Project Manager</b>	\$200
<b>Lead Consultant</b>	\$250
<b>Senior Solution Architect</b>	\$250
<b>Senior Infrastructure Architect</b>	\$200
<b>Digital Transformation Analyst</b>	\$175

Contractor Initials: MS

Oil and Gas Commission (authorized initials): 



## SCHEDULE B Fees and Expenses

This Schedule forms part of the agreement.

Contract No: 21422002

2. The Contractor should submit to the Commission, monthly, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.
3. After receipt by the Commission of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.
4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is **\$200,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): [Signature]



This Schedule forms part of the agreement.

Contract No: 21422002

**Insurance:**

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Commission:
  - (a) Commercial General Liability in an amount not less than **\$2,000,000** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
    - (i) include the Commission as an additional insured,
    - (ii) be endorsed to provide the Commission with 30 days advance written notice of cancellation or material change, and
    - (iii) include a cross liability clause;
2. All insurance described in section 1 of this Schedule must:
  - (a) be primary; and
  - (b) not require the sharing of any loss by any insurer of the Commission.
3. The Contractor must provide the Commission with evidence of all required insurance as follows:
  - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Commission evidence of all required insurance in the form of a completed Certificate of Insurance;
  - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Commission within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Commission of British Columbia Certificate of Insurance; and
  - (c) despite paragraph (a) or (b) above, if requested by the Commission at any time, the Contractor must provide to the Commission certified copies of the required insurance policies.
4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): [Signature]

This Schedule forms part of the agreement.

Contract No: 21422002

### Definitions

1. In this Schedule,
  - (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
  - (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
  - (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Commission and the Contractor dealing with the same subject matter as the Agreement.

### Purpose

2. The purpose of this Schedule is to:
  - (a) enable the Commission to comply with its statutory obligations under the Act with respect to personal information; and
  - (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

### Collection of personal information

3. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
  - (a) the purpose for collecting it;
  - (b) the legal authority for collecting it; and
  - (c) the title, business address and business telephone number of the person designated by the Commission to answer questions about the Contractor's collection of personal information.

### Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Commission to make a decision that directly affects the individual the information is about.

### Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission unless the Agreement expressly requires the Contractor to provide such access and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

### Correction of personal information

8. Within 5 business days of receiving a written direction from the Commission to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
9. When issuing a written direction under section 8, the Commission must advise the Contractor of the date the correction request to which the direction relates was received by the Commission in order that the Contractor may comply with section 10.
10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Commission, the Contractor disclosed the information being corrected or annotated.
11. If the Contractor receives a request for correction of personal information from a person other than the Commission, the Contractor must promptly advise the person to make the request to the Commission and, if the Commission has advised the Contractor of the name or title and contact information of an official of the Commission to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

### Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

### Storage and access to personal information

13. Unless the Commission otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Contractor Initials:

*MS*

Oil and Gas Commission (authorized initials):

*[Signature]*

This Schedule forms part of the agreement.

Contract No: 21422002

### Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Commission in writing to dispose of it or deliver it as specified in the direction.

### Use of personal information

15. Unless the Commission otherwise directs in writing, the Contractor may only use personal information if that use is:
- (a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and
  - (b) in accordance with section 13.

### Disclosure of personal information

16. Unless the Commission otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Commission if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
17. Unless the Agreement otherwise specifies or the Commission otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

### Inspection of personal information

18. In addition to any other rights of inspection the Commission may have under the Agreement or under statute, the Commission may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

### Compliance with the Act and directions

19. The Contractor must in relation to personal information comply with:
- (a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
  - (b) any direction given by the Commission under this Schedule.
20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

### Notice of non-compliance

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Commission of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

### Termination of Agreement

22. In addition to any other rights of termination which the Commission may have under the Agreement or otherwise at law, the Commission may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

### Interpretation

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
26. If a provision of the Agreement (including any direction given by the Commission under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): AD



CONTRACT AMENDMENT #1

THIS AMENDMENT MADE THIS 26<sup>th</sup> DAY OF SEPTEMBER 2022

BETWEEN:

OIL AND GAS COMMISSION (HEREIN CALLED THE "COMMISSION")  
OF THE FIRST PART

AND:

GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")  
OF THE SECOND PART

WITNESSETH THAT WHEREAS:

- A. The parties hereto entered into a General Services Agreement identified as Contract No. 21422002 for a term which commenced on February 1, 2022 and is scheduled to end on March 31, 2024;
- B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:


- 1. This amendment is made effective October 1, 2022.
- 2. Maximum Fees will increase by \$122,000 from \$200,000 to \$322,000. Clauses 1 and 4 will be removed and replaced with the following:
  - 1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **\$322,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Role	Rate (per hour)
Senior Project Manager	\$200
Lead Consultant	\$250
Senior Solution Architect	\$250
Senior Infrastructure Architect	\$200
Digital Transformation Analyst	\$175

**CONTRACT AMENDMENT #1**

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is **\$322,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.
  
5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

**IN WITNESS WHEREOF** the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the <u>28th</u> day of September 2022 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the <u>27</u> day of September 2022 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	<i>Michael Schweitzer</i>
Signature	Signature
<b>Ab Dosil</b>	<b>Michael Schweitzer</b>
Print Name	Print Name



CONTRACT AMENDMENT #2

THIS AMENDMENT MADE THIS 2<sup>nd</sup> DAY OF FEBRUARY 2023

BETWEEN:

OIL AND GAS COMMISSION (HEREIN CALLED THE "COMMISSION")  
OF THE FIRST PART

AND:

GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")  
OF THE SECOND PART

WITNESSETH THAT WHEREAS:

- A. The parties hereto entered into a General Services Agreement identified as Contract No. 21422002 for a term which commenced on February 1, 2022 and is scheduled to end on March 31, 2024;
- B. **AND WHEREAS** the parties have agreed to modify the Agreement.

NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:


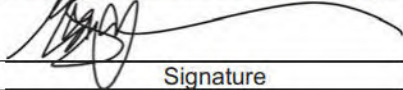
- 1. This amendment is made effective February 1, 2023.
- 2. Maximum Fees will increase by \$38,000 from \$322,000 to \$360,000. Clauses 1 and 4 will be removed and replaced with the following:
  - 1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **\$360,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Role	Rate (per hour)
Senior Project Manager	\$200
Lead Consultant	\$250
Senior Solution Architect	\$250
Senior Infrastructure Architect	\$200
Digital Transformation Analyst	\$175

**CONTRACT AMENDMENT #2**

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is **\$360,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.
  
5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

**IN WITNESS WHEREOF** the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the <u>07</u> day of February 2023 on behalf of the Oil and Gas Commission by its duly authorized representative:	SIGNED AND DELIVERED on the <u>07</u> day of February 2023 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
<b>Ab Dosil</b>	<b>Michael Schweitzer</b>
Print Name	Print Name

CONTRACT AMENDMENT #3

THIS AMENDMENT MADE THIS 8<sup>th</sup> DAY OF MAY 2023

BETWEEN:

BC ENERGY REGULATOR (HEREIN CALLED THE "REGULATOR")

OF THE FIRST PART

AND:

GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")

OF THE SECOND PART

WITNESSETH THAT WHEREAS:

- A. The parties hereto entered into a General Services Agreement identified as Contract No. 21422002 for a term which commenced on February 1, 2022 and is scheduled to end on March 31, 2024;
- B. **AND WHEREAS** the parties have agreed to modify the Agreement.

**NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:**

- 1. This amendment is made effective May 1, 2023.
- 2. Maximum Fees will increase by \$200,000 from \$360,000 to \$560,000. Clauses 1 and 4 will be removed and replaced with the following:
  - 1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **\$560,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Role	Rate (per hour)
Senior Project Manager	\$200
Lead Consultant	\$250
Senior Solution Architect	\$250
Senior Infrastructure Architect	\$200
Digital Transformation Analyst	\$175

- 4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is **\$560,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.



CONTRACT AMENDMENT #3

5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

IN WITNESS WHEREOF the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the <u>11<sup>th</sup></u> day of May 2023 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the <u>10</u> day of May 2023 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
<b>Ab Dosil</b>	<b>Michael Schweitzer</b>
Print Name	Print Name



**CONTRACT No. 21422002**

**CONTRACT AMENDMENT #4**

**THIS AMENDMENT MADE THIS 26<sup>th</sup> DAY OF APRIL 2024**

**BETWEEN:**

**BC ENERGY REGULATOR (HEREIN CALLED THE "REGULATOR")**

**OF THE FIRST PART**

**AND:**

**GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")**

**OF THE SECOND PART**

**WITNESSETH THAT WHEREAS:**

- A. The parties hereto entered into an Information Technology Professional Services Agreement identified as Contract No. 21422002 for a term which commenced on February 1, 2022, and was scheduled to end on March 31, 2024;
- B. **AND WHEREAS** the parties have agreed to modify the Agreement.

**NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:**

- 1. This amendment is made effective April 1, 2024.
- 2. The term of the Agreement is extended to March 31, 2025. The term described in Schedule "A" is deleted and replaced with:  
  - The term of this Agreement commences on February 1, 2022, and ends on March 31, 2025.
- 3. Maximum Fees will increase by \$220,000 from \$560,000 to \$780,000. Clauses 1 and 4 will be removed and replaced with the following:
  - 1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **\$780,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Activity and Role	Cost
Digital Transformation Analyst	\$175 per hour
Solution and Infrastructure Architect	\$200 per hour
Project Manager	\$200 per hour


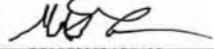


**CONTRACT No. 21422002**

**CONTRACT AMENDMENT #4**

- 4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is **\$780,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.
  
- 5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

**IN WITNESS WHEREOF** the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the <u>29<sup>th</sup></u> day of April 2024 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the <u>26</u> day of April 2024 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
<b>Sara Dickinson</b>	<b>Michael Schweitzer</b>
Print Name	Print Name

# Department and Project Sites

BC Energy Regulator – Statement of Work



BC Energy Regulator — Department and Project Sites

# Statement of Work

March 26, 2024

## Confidentiality and Warranty

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Gravity Union Solution Limited.

The opinions expressed are in good faith and while every care has been taken in preparing these documents, Gravity Union makes no representations and gives no warranties of whatever nature in respect of these documents, including and not limited to the accuracy or completeness of any information, facts and/or opinions contained therein.

## Validity

This Statement of Work shall remain valid for 60 days.

Gold Certified

Collabware Partner



Gold

Microsoft Partner



## Table of Contents

Introduction .....	3
Proposed Scope and Effort .....	3
Estimated Project Cost.....	4
Rates .....	4
Estimated Cost .....	4
Payments.....	4
Proposed Team .....	4
Assumptions.....	5
Support .....	5
Microsoft Gold Partner .....	5
Travel and Expenses .....	5
Cancellation .....	5
Change Orders .....	6
Payment .....	6
Authorization .....	6

## Introduction

BC Energy Regulator engaged Gravity Union to design and configure SharePoint Online department and project sites for their organization. As the rollouts are still in progress, BCER requested Gravity Union to continue the rollout work of the SharePoint Departments, Teams, and Project sites and the related M365 infrastructure.

## Proposed Scope and Effort

Gravity Union will design, configure, test and rollout nine additional department and project sites.

Based on the proposed effort and assumptions listed, below is the estimated cost.

Activity	Cost
Current state assessment, business requirements gathering, content discovery and audit, card sort exercise	
Iterative prototype build and test, solution refinements	
Migration planning and migration support	
End-user training, solution specific training, dry run of new solution, go-live support	
Retrospective and Transition to Operations	
Team meetings and check-ins for Digital Transformation Analyst and Solution Architect	
Project Management (at \$200 per hour)	
<b>Total</b>	<b>\$200,000</b>

## Estimated Project Cost

### Rates

Gravity Union’s standard rates range between \$175 and \$250 per hour. Please see the rates table below for further details:

Activity and Role	Cost
Digital Transformation Analyst	\$175 per hour
Solution and Infrastructure Architect	\$200 per hour
Project Manager	\$200 per hour

### Estimated Cost

Gravity Union proposes a Time & Materials project budget targeting \$200,000 +/- 25% where BC Energy Regulator is only billed for costs incurred, using the estimated costs below as our target budget. Any cost actuals beyond this budget would require prior approval before work execution or billing.

### Payments

Invoices would be submitted at the end of each month, for hours worked during that month, due upon receipt.

## Proposed Team

- ☑ Pauline Richer, Digital Transformation Analyst
- ☑ Denis Boico, Solution and Infrastructure Architect
- ☑ Thabata Granja, Project Manager
- ☑ Michael Schweitzer, Account Manager



## Assumptions

- ☑ BCER will provide Gravity Union with relevant SharePoint account and access.
- ☑ The nine departments/groups will be determined. For this SOW, nine departments/groups are in scope.

## Support

With resources across Canada, Gravity Union’s standard support from 6:00am PT to 6:00 pm PT. Gravity Union can perform work outside of these hours when scheduled in advance and can negotiate support agreements for organizations beyond our regular hours on an as-needed basis.

## Microsoft Gold Partner

As a Microsoft Gold Partner, we have access to resources and support directly from Microsoft to troubleshoot problems and issues and can escalate within Microsoft for support.

## Travel and Expenses

At current, we do not anticipate any travel costs; however, travel costs and expenses will be itemized separately from hours for billing. There will be no mark-ups on travel costs and fees incurred.

## Cancellation

The BC Energy Regulator is free to cancel this arrangement at any time. All time worked up to the notification of cancellation will be billed and owed to Gravity Union by BC Energy Regulator.

## Change Orders

Proposed changes or extensions to the contracted work statement(s) must be in writing and approved by both BC Energy Regulator and Gravity Union before the commencement of work. Additional fees will be invoiced in the regular billing cycle described below.

## Payment

The BC Energy Regulator will be billed at the end of each month for hours worked with payment due upon receipt. Included with each invoice will be a breakdown of hours with descriptions.

## Authorization

By signing the below, all parties agree to enter into a contract for services as described in this document.

BC Energy Regulator

Name (printed) Derek Mathews

Date March 28, 2024

Signature 

Gravity Union Solutions Limited

Name (printed) Michael Schweitzer

Date \_\_\_\_\_

Signature \_\_\_\_\_



# Information Technology Professional Service Agreement

For Administration Purpose Only

Account No: 52050-214-000003

Solicitation No: Quoted

Contract No: 21424001

BETWEEN	AND
<b>British Columbia Energy Regulator also referred to as "Regulator"</b>	<b>Gravity Union Solutions Limited also referred to as the "Contractor"</b>
(the "Regulator", "we", "us", or "our" as applicable) at the following address:	(the "Contractor", "you", or "your" as applicable) at the following address:
2950 Jutland Road Victoria, BC V8T 5K2	1240 - 605 Robson Street Vancouver, BC V6B 5J3
Phone number: 250.419.4400 Email: <a href="mailto:procurement@bc-er.ca">procurement@bc-er.ca</a>	Phone Number: 604.782.1507 Email: <a href="mailto:mschweitzer@gravityunion.com">mschweitzer@gravityunion.com</a>

**THE BC ENERGY REGULATOR AND THE CONTRACTOR AGREE TO THE TERMS CONTAINED WITHIN THIS DOCUMENT AND IN THE SCHEDULES OUTLINED BELOW.**

**SCHEDULE A – list of Services:** SharePoint Operational Portal Support Services (See attached)

**Term: Start Date:** May 1, 2023

**End Date:** March 31, 2024

<b>SCHEDULE B - FEES AND EXPENSES:</b>	
Fees: \$ 50,000	Expenses: \$
Billing Date(s): <b>Monthly / Upon Invoice</b>	Maximum Amount: <b>\$ 50,000</b>

**SCHEDULE C - APPROVED SUBCONTRACTOR(S):**

N/A

**SCHEDULE D - INSURANCE:**

N/A

**SCHEDULE E – PRIVACY PROTECTION:**



N/A

**SCHEDULE F – ADDITIONAL TERMS:**

N/A

**SCHEDULE G – SECURITY:**

N/A

SIGNED AND DELIVERED on the <u>5th</u> day of May 2023 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the <u>5th</u> day of May 2023 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signer: <b>DG RATH...</b>	Signature
<b>Derek Mathews</b>	<b>Michael Schweitzer</b>
Print Name	Print Name

**READ TERMS ON THE FOLLOWING PAGES**

# TERMS OF INFORMATION TECHNOLOGY PROFESSIONAL SERVICE AGREEMENT

## 1 DEFINITIONS

### General

- 1.1 In this Agreement, unless the context otherwise requires:
- (a) "Business Day" means a day, other than a Saturday or Sunday, on which Provincial government offices are open for normal business in British Columbia;
  - (b) "Incorporated Material" means any material in existence prior to the start of the Term or developed independently of this Agreement, and that is incorporated or embedded in the Produced Material by the Contractor or a Subcontractor;
  - (c) "Material" means the Produced Material and the Received Material;
  - (d) "Produced Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are produced or provided by the Contractor or a Subcontractor and includes the Incorporated Material;
  - (e) "Received Material" means records, software and other material, whether complete or not, that, as a result of this Agreement, are received by the Contractor or a Subcontractor from the Regulator or any other person;
  - (f) "Services" means the services described in Part 2 of Schedule A;
  - (g) "Subcontractor" means a person described in paragraph (a) or (b) of section 13.4; and
  - (h) "Term" means the term of the Agreement described in Part 1 of Schedule A subject to that term ending earlier in accordance with this Agreement.

### Meaning of "record"

- 1.2 The definition of "record" in the *Interpretation Act* is incorporated into this Agreement and "records" will bear a corresponding meaning.

## 2 SERVICES

### Provision of services

- 2.1 The Contractor must provide the Services in accordance with this Agreement.

### Term

- 2.2 Regardless of the date of execution or delivery of this Agreement, the Contractor must provide the Services during the Term.

### Supply of various items

- 2.3 Unless the parties otherwise agree in writing, the Contractor must supply and pay for all labour, materials, equipment, tools, facilities, approvals and licenses necessary or advisable to perform the Contractor's obligations under this Agreement, including the license under section 6.4.

### Standard of care

- 2.4 Unless otherwise specified in this Agreement, the Contractor must perform the Services to a standard of care, skill, and diligence maintained by persons providing, on a commercial basis, services similar to the Services.

### Standards in relation to persons performing Services

- 2.5 The Contractor must ensure that all persons employed or retained to perform the Services are qualified and competent to perform them and are properly trained, instructed and supervised.

### Instructions by Regulator

- 2.6 The Regulator may from time to time give the Contractor reasonable instructions (in writing or otherwise) as to the performance of the Services. The Contractor must comply with those instructions, but, unless otherwise specified in this Agreement, the Contractor may determine the manner in which the instructions are carried out.

### Confirmation of non-written instructions

- 2.7 If the Regulator provides an instruction under section 2.6 other than in writing, the Contractor may request that the instruction be confirmed by the Regulator in writing, which request the Regulator must comply with as soon as it is reasonably practicable to do so.

### Effectiveness of non-written instructions

- 2.8 Requesting written confirmation of an instruction under section 2.7 does not relieve the Contractor from complying with the instruction at the time the instruction was given.

### Applicable laws

- 2.9 In the performance of the Contractor's obligations under this Agreement, the Contractor must comply with all applicable laws.

## 3 PAYMENT

### Fees and expenses

- 3.1 If the Contractor complies with this Agreement, then the Regulator must pay to the Contractor at the times and on the conditions set out in Schedule B:
- (a) the fees described in that Schedule;
  - (b) the expenses, if any, described in that Schedule if they are supported, where applicable, by proper receipts and, in the Regulator's opinion, are necessarily incurred by the Contractor in providing the Services; and
  - (c) any applicable taxes payable by the Regulator under law or agreement with the relevant taxation authorities on the fees and expenses described in paragraphs (a) and (b).

The Regulator is not obliged to pay to the Contractor more than the "Maximum Amount" specified in Schedule B on account of fees and expenses.

### Statements of accounts

- 3.2 In order to obtain payment of any fees and expenses under this Agreement, the Contractor must submit to the Regulator a written statement of account in a form satisfactory to the Regulator upon completion of the Services or at other times described in Schedule B.

### Withholding of amounts

- 3.3 Without limiting section 9.1, the Regulator may withhold from any payment due to the Contractor an amount sufficient to indemnify in whole or in part the Regulator and its employees and agents against any liens or other third-party claims that have arisen or could arise in connection with the provision of the Services. An amount withheld under this section must be promptly paid by the Regulator to the Contractor upon the basis for withholding the amount having been fully resolved to the satisfaction of the Regulator.

### Appropriation

- 3.4 The Regulator's obligation to pay money to the Contractor is subject to the *Financial Administration Act*, which makes that obligation subject to an appropriation being available in the fiscal year of the Regulator during which payment becomes due.

### Currency

- 3.5 Unless otherwise specified in this Agreement, all references to money are to Canadian dollars.

### Non-resident income tax

- 3.6 If the Contractor is not a resident in Canada, the Contractor acknowledges that the Regulator may be required by law to withhold income tax from the fees described in Schedule B and then to remit that tax to the Receiver General of Canada on the Contractor's behalf.

### Prohibition against committing money

- 3.7 Without limiting section 13.10(a), the Contractor must not in relation to performing the Contractor's obligations under this Agreement commit or purport to commit the Regulator to pay any money except as may be expressly provided for in this Agreement.

### Refunds of taxes

- 3.8 The Contractor must:
- (a) apply for, and use reasonable efforts to obtain, any available refund, credit, rebate or remission of federal, provincial or other tax or duty imposed on the Contractor as a result of this Agreement that the Regulator has paid or reimbursed to the Contractor or agreed to pay or reimburse to the Contractor under this Agreement; and
  - (b) immediately on receiving, or being credited with, any amount applied for under paragraph (a), remit that amount to the Regulator.

## 4 REPRESENTATIONS AND WARRANTIES

- 4.1 As at the date this Agreement is executed and delivered by, or on behalf of, the parties, the Contractor represents and warrants to the Regulator as follows:

- (a) except to the extent the Contractor has previously disclosed otherwise in writing to the Regulator,
  - (i) all information, statements, documents and reports furnished or submitted by the Contractor to the Regulator in connection with this Agreement (including as part of any competitive process resulting in this Agreement being entered into) are in all material respects true and correct,
  - (ii) the Contractor has sufficient trained staff, facilities, materials, appropriate equipment and approved subcontractual or other agreements in place and available to enable the Contractor to fully perform the Services and to grant any licenses under this Agreement, and
  - (iii) the Contractor holds all permits, licenses, approvals and statutory authorities issued by any government or government agency that are necessary for the performance of the Contractor's obligations under this Agreement; and

Contractor Initials: MS

Oil and Gas Commission (authorized initials): DM

# TERMS OF INFORMATION TECHNOLOGY PROFESSIONAL SERVICE AGREEMENT

- (b) if the Contractor is not an individual,
- (i) the Contractor has the power and capacity to enter into this Agreement and to observe, perform and comply with the terms of this Agreement and all necessary corporate or other proceedings have been taken and done to authorize the execution and delivery of this Agreement by, or on behalf of, the Contractor, and this Agreement has been legally and properly executed by, or on behalf of, the Contractor and is legally binding upon and enforceable against the Contractor in accordance with its terms except as enforcement may be limited by bankruptcy, insolvency or other laws affecting the rights of creditors generally and except that equitable remedies may be granted only in the discretion of a court of competent jurisdiction.

## 5 PRIVACY, SECURITY AND CONFIDENTIALITY

### Privacy

- 5.1 The Contractor must comply with the Privacy Protection Schedule attached as Schedule E.

### Security

- 5.2 The Contractor must:
- (a) make reasonable security arrangements to protect the Material from unauthorized access, collection, use, disclosure, alteration or disposal; and
- (b) comply with the Security Schedule attached as Schedule G.

### Confidentiality

- 5.3 The Contractor must treat as confidential all information in the Material and all other information accessed or obtained by the Contractor or a Subcontractor (whether verbally, electronically or otherwise) as a result of this Agreement, and not permit its disclosure or use without the Regulator's prior written consent except:
- (a) as required to perform the Contractor's obligations under this Agreement or to comply with applicable laws;
- (b) if it is information that is generally known to the public other than as result of a breach of this Agreement; or
- (c) if it is information in any Incorporated Material.

### Public announcements

- 5.4 Any public announcement relating to this Agreement will be arranged by the Regulator and, if such consultation is reasonably practicable, after consultation with the Contractor.

### Restrictions on promotion

- 5.5 The Contractor, must not, without the prior written approval of the Regulator, refer for promotional purposes to the Regulator being a customer of the Contractor or the Regulator having entered into this Agreement.

## 6 MATERIAL AND INTELLECTUAL PROPERTY

### Access to Material

- 6.1 If the Contractor receives a request for access to any of the Material from a person other than the Regulator, and this Agreement does not require or authorize the Contractor to provide that access, the Contractor must promptly advise the person to make the request to the Regulator.

### Ownership and delivery of Material

- 6.2 The Regulator exclusively owns all property rights in the Material which are not intellectual property rights. The Contractor must deliver any Material to the Regulator immediately upon the Regulator's request.

### Matters respecting intellectual property

- 6.3 The Regulator exclusively owns all intellectual property rights, including copyright, in:
- (a) Received Material that the Contractor receives from the Regulator; and
- (b) Produced Material, other than any Incorporated Material.

Upon the Regulator's request, the Contractor must deliver to the Regulator documents satisfactory to the Regulator that irrevocably waive in the Regulator's favour any moral rights which the Contractor (or employees of the Contractor) or a Subcontractor (or employees of a Subcontractor) may have in the Produced Material and that confirm the vesting in the Regulator of the copyright in the Produced Material, other than any Incorporated Material.

### Rights in relation to Incorporated Material

- 6.4 Upon any Incorporated Material being embedded or incorporated in the Produced Material and to the extent that it remains so embedded or incorporated, the Contractor grants to the Regulator:
- (a) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to exercise, in respect of that Incorporated Material, the rights set out in the *Copyright Act* (Canada), including the right to use, reproduce, modify, publish and distribute that Incorporated Material; and
- (b) the right to sublicense or assign to third-parties any or all of the rights granted to the Regulator under section 6.4(a).

### Right of Regulator to negotiate license of Produced Material

- 6.5 After the end of the Term, the Regulator in its sole discretion, may negotiate with the Contractor to provide the Contractor a license (which may be

exclusive or non-exclusive) for the Contractor to use, reproduce, modify or distribute some or all of the Produced Material.

## 7 RECORDS AND REPORTS

### Work reporting

- 7.1 Upon the Regulator's request, the Contractor must fully inform the Regulator of all work done by the Contractor or a Subcontractor in connection with providing the Services.

### Time and expense records

- 7.2 If Schedule B provides for the Contractor to be paid fees at a daily or hourly rate or for the Contractor to be paid or reimbursed for expenses, the Contractor must maintain time records and books of account, invoices, receipts and vouchers of expenses in support of those payments, in form and content satisfactory to the Regulator. Unless otherwise specified in this Agreement, the Contractor must retain such documents for a period of not less than seven years after this Agreement ends.

## 8 AUDIT

- 8.1 In addition to any other rights of inspection the Regulator may have under statute or otherwise, the Regulator may at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect and, at the Regulator's discretion, copy any of the Material and the Contractor must permit, and provide reasonable assistance to, the exercise by the Regulator of the Regulator's rights under this section.

## 9 INDEMNITY AND INSURANCE

### Indemnity

- 9.1 The Contractor must indemnify and save harmless the Regulator and the Regulator's employees and agents from any loss, claim (including any claim of infringement of third-party intellectual property rights), damage award, action, cause of action, cost or expense that the Regulator or any of the Regulator's employees or agents may sustain, incur, suffer or be put to at any time, either before or after this Agreement ends, (each a "Loss") to the extent the Loss is directly or indirectly caused or contributed to by
- (a) any act or omission by the Contractor or by any of the Contractor's agents, employees, officers, directors or Subcontractors in connection with this Agreement; or
- (b) any representation or warranty of the Contractor being or becoming untrue or incorrect.

### Monetary limitations of indemnity

- 9.2 The indemnification by the Contractor pursuant to section 9.1 is limited to:
- (a) \$2,000,000 per Loss; and
- (b) \$4,000,000 in the aggregate for all Losses.

### Exceptions to monetary limitations

- 9.3 The limitations set out in section 9.2 do not apply to a Loss resulting from or relating to any of the following:
- (a) bodily injury or damage to real property or tangible personal property;
- (b) third-party intellectual property rights; or
- (c) a breach of section 5.1, 5.2, 5.3 or 6.1 of this Agreement.

### Regulator to notify Contractor of Loss

- 9.4 To claim indemnification for a Loss pursuant to section 9.1, the Regulator must notify the Contractor in writing of the Loss as soon as reasonably practicable after the Regulator becomes aware of the Loss provided that a failure by the Regulator to provide such notification will not invalidate the claim unless the Contractor is materially prejudiced by that failure.

### Third-party intellectual property infringement claims

- 9.5 If the Loss is on the basis of a third-party claim that any element of the Material infringes the intellectual property rights of any person,
- (a) then, without limiting section 9.1, the Contractor must defend the Regulator against that claim at the Contractor's expense and the Contractor must pay all associated costs, damages and legal fees that a court or arbitrator finally awards or are included in a settlement agreed to by the Contractor; and
- (b) the Regulator must cooperate with the Contractor in the defence of the claim and, where appropriate in the discretion of the Regulator, will allow the Contractor to appoint and instruct counsel and otherwise control the defence and any related settlement negotiations.

### Insurance

- 9.6 The Contractor must comply with the Insurance Schedule attached as Schedule D.

### Workers compensation

- 9.7 Without limiting the generality of section 2.9, the Contractor must comply with, and must ensure that any Subcontractors comply with, all applicable occupational health and safety laws in relation to the performance of the Contractor's obligations under this Agreement, including the *Workers Compensation Act* in British Columbia or similar laws in other jurisdictions.

### Personal optional protection

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

# TERMS OF INFORMATION TECHNOLOGY PROFESSIONAL SERVICE AGREEMENT

- 9.8 The Contractor must apply for and maintain personal optional protection insurance (consisting of income replacement and medical care coverage) during the Term at the Contractor's expense if:
- (a) the Contractor is an individual or a partnership of individuals and does not have the benefit of mandatory workers compensation coverage under the *Workers Compensation Act* or similar laws in other jurisdictions; and
  - (b) such personal optional protection insurance is available for the Contractor from WorkSafeBC or other sources.

#### Evidence of coverage

- 9.9 Within 10 Business Days of being requested to do so by the Regulator, the Contractor must provide the Regulator with evidence of the Contractor's compliance with sections 9.7 and 9.8.

## 10 FORCE MAJEURE

#### Definitions relating to force majeure

- 10.1 In this section and sections 10.2 and 10.3:
- (a) "Event of Force Majeure" means one of the following events:
    - (i) a natural disaster, fire, flood, storm, epidemic or power failure;
    - (ii) a war (declared and undeclared), insurrection or act of terrorism or piracy;
    - (iii) a strike (including illegal work stoppage or slowdown) or lockout, or
    - (iv) a freight embargo if the event prevents a party from performing the party's obligations in accordance with this Agreement and is beyond the reasonable control of that party; and
  - (b) "Affected Party" means a party prevented from performing the party's obligations in accordance with this Agreement by an Event of Force Majeure.

#### Consequence of Event of Force Majeure

- 10.2 An Affected Party is not liable to the other party for any failure or delay in the performance of the Affected Party's obligations under this Agreement resulting from an Event of Force Majeure and any time periods for the performance of such obligations are automatically extended for the duration of the Event of Force Majeure provided that the Affected Party complies with the requirements of section 10.3.

#### Duties of Affected Party

- 10.3 An Affected Party must promptly notify the other party in writing upon the occurrence of the Event of Force Majeure and make all reasonable efforts to prevent, control or limit the effect of the Event of Force Majeure so as to resume compliance with the Affected Party's obligations under this Agreement as soon as possible.

## 11 DEFAULT AND TERMINATION

#### Definitions relating to default and termination

- 11.1 In this section and sections 11.2 to 11.4:
- (a) "Event of Default" means any of the following:
    - (i) an Insolvency Event;
    - (ii) the Contractor fails to perform any of the Contractor's obligations under this Agreement, or
    - (iii) any representation or warranty made by the Contractor in this Agreement is untrue or incorrect; and
  - (b) "Insolvency Event" means any of the following:
    - (i) an order is made, a resolution is passed or a petition is filed, for the Contractor's liquidation or winding up;
    - (ii) the Contractor commits an act of bankruptcy, makes an assignment for the benefit of the Contractor's creditors or otherwise acknowledges the Contractor's insolvency;
    - (iii) a bankruptcy petition is filed or presented against the Contractor or a proposal under the *Bankruptcy and Insolvency Act* (Canada) is made by the Contractor;
    - (iv) a compromise or arrangement is proposed in respect of the Contractor under the *Companies' Creditors Arrangement Act* (Canada);
    - (v) a receiver or receiver-manager is appointed for any of the Contractor's property; or
    - (vi) the Contractor ceases, in the Regulator's reasonable opinion, to carry on business as a going concern.

#### Regulator's options on default

- 11.2 On the happening of an Event of Default, or at any time thereafter, the Regulator may, at its option, elect to do any one or more of the following:
- (a) by written notice to the Contractor, require that the Event of Default be remedied within a time period specified in the notice;
  - (b) pursue any remedy or take any other action available to it at law or in equity; or
  - (c) by written notice to the Contractor, terminate this Agreement with immediate effect or on a future date specified in the notice, subject to the expiration of any time period specified under section 11.2(a).

#### Delay not a waiver

- 11.3 No failure or delay on the part of the Regulator to exercise its rights in relation to an Event of Default will constitute a waiver by the Regulator of such rights.

#### Regulator's right to terminate other than for default

- 11.4 In addition to the Regulator's right to terminate this Agreement under section 11.2(c) on the happening of an Event of Default, the Regulator may terminate this Agreement for any reason by giving at least 10 days' written notice of termination to the Contractor.

#### Payment consequences of termination

- 11.5 Unless Schedule B otherwise provides, if the Regulator terminates this Agreement under section 11.4:
- (a) the Regulator must, within 30 days of such termination, pay to the Contractor any unpaid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that was completed to the Regulator's satisfaction before termination of this Agreement; and
  - (b) the Contractor must, within 30 days of such termination, repay to the Regulator any paid portion of the fees and expenses described in Schedule B which corresponds with the portion of the Services that the Regulator has notified the Contractor in writing was not completed to the Regulator's satisfaction before termination of this Agreement.

#### Discharge of liability

- 11.6 The payment by the Regulator of the amount described in section 11.5(a) discharges the Regulator from all liability to make payments to the Contractor under this Agreement.

#### Notice in relation to Events of Default

- 11.7 If the Contractor becomes aware that an Event of Default has occurred or anticipates that an Event of Default is likely to occur, the Contractor must promptly notify the Regulator of the particulars of the Event of Default or anticipated Event of Default. A notice under this section as to the occurrence of an Event of Default must also specify the steps the Contractor proposes to take to address, or prevent recurrence of, the Event of Default. A notice under this section as to an anticipated Event of Default must specify the steps the Contractor proposes to take to prevent the occurrence of the anticipated Event of Default.

## 12 DISPUTE RESOLUTION

#### Dispute resolution process

- 12.1 In the event of any dispute between the parties arising out of or in connection with this Agreement, the following dispute resolution process will apply unless the parties otherwise agree in writing:
- (a) the parties must initially attempt to resolve the dispute through collaborative negotiation;
  - (b) if the dispute is not resolved through collaborative negotiation within 15 Business Days of the dispute arising, the parties must then attempt to resolve the dispute through mediation under the rules of the Mediate BC Society; and
  - (c) if the dispute is not resolved through mediation within 30 Business Days of the commencement of mediation, the dispute must be referred to and finally resolved by arbitration under the *Arbitration Act*.

#### Location of arbitration or mediation

- 12.2 Unless the parties otherwise agree in writing, an arbitration or mediation under section 12.1 will be held in Victoria, British Columbia.

#### Costs of arbitration or mediation

- 12.3 Unless the parties otherwise agree in writing or, in the case of an arbitration, the arbitrator otherwise orders, the parties must share equally the costs of a arbitration or mediation under section 12.1 other than those costs relating to the production of expert evidence or representation by counsel.

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

# TERMS OF INFORMATION TECHNOLOGY PROFESSIONAL SERVICE AGREEMENT

## 13 MISCELLANEOUS

### Delivery of notices

- 13.1 Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows:
- (a) by email to the addressee's email specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a Business Day, in which cases it will be deemed to be received on the next following Business Day;
  - (b) by hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or
  - (c) by prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth Business Day after its mailing.

### Change of address or email

- 13.2 Either party may from time to time give notice to the other party of a substitute address or email, which from the date such notice is given will supersede for purposes of section 13.1 any previous address or email specified for the party giving the notice.

### Assignment

- 13.3 The Contractor must not assign any of the Contractor's rights or obligations under this Agreement without the Regulator's prior written consent. Upon providing written notice to the Contractor, the Regulator may assign to any person any of the Regulator's rights under this Agreement and may assign to any "government corporation", as defined in the *Financial Administration Act*, any of the Regulator's obligations under this Agreement.

### Subcontracting

- 13.4 The Contractor must not subcontract any of the Contractor's obligations under this Agreement to any person without the Regulator's prior written consent, excepting persons listed in the attached Schedule C. No subcontract, whether consented to or not, relieves the Contractor from any obligations under this Agreement. The Contractor must ensure that:
- (a) any person retained by the Contractor to perform obligations under this Agreement; and
  - (b) any person retained by a person described in paragraph (a) to perform those obligations fully complies with this Agreement in performing the subcontracted obligations.

### Waiver

- 13.5 A waiver of any term or breach of this Agreement is effective only if it is in writing and signed by, or on behalf of, the waiving party and is not a waiver of any other term or breach.

### Modifications

- 13.6 No modification of this Agreement is effective unless it is in writing and signed by, or on behalf of, the parties.

### Entire agreement

- 13.7 This Agreement (including any modification of it) constitutes the entire agreement between the parties as to performance of the Services.

### Survival of certain provisions

- 13.8 Sections 2.9, 3.1 to 3.4, 3.7, 3.8, 5.1 to 5.5, 6.1 to 6.5, 7.1, 7.2, 8.1, 9.1 to 9.6, 9.9, 10.1 to 10.3, 11.2, 11.3, 11.5, 11.6, 12.1 to 12.3, 13.1, 13.2, 13.8, and 13.10, any accrued but unpaid payment obligations, and any other sections of this Agreement (including schedules) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely subject to any applicable limitation period prescribed by law, even after this Agreement ends.

### Schedules

- 13.9 The schedules to this Agreement (including any appendices or other documents attached to, or incorporated by reference into, those schedules) are part of this Agreement.

### Independent contractor

- 13.10 In relation to the performance of the Contractor's obligations under this Agreement, the Contractor is an independent contractor and not:
- (a) an employee or partner of the Regulator; or
  - (b) an agent of the Regulator except as may be expressly provided for in this Agreement.
- The Contractor must not act or purport to act contrary to this section.

### Personnel not to be employees of Regulator

- 13.11 The Contractor must not do anything that would result in personnel hired or used by the Contractor or a Subcontractor in relation to providing the Services being considered employees of the Regulator.

### Key Personnel

- 13.12 If one or more individuals are specified as "Key Personnel" of the Contractor in Part 4 of Schedule A, the Contractor must cause those individuals to perform the Services on the Contractor's behalf, unless the Regulator otherwise approves in writing, which approval must not be unreasonably withheld.

### Pertinent information

- 13.13 The Regulator must make available to the Contractor all information in the Regulator's possession which the Regulator considers pertinent to the performance of the Services.

### Conflict of interest

- 13.14 The Contractor must not provide any services to any person in circumstances which, in the Regulator's reasonable opinion, could give rise to a conflict of interest between the Contractor's duties to that person and the Contractor's duties to the Regulator under this Agreement.

### Time

- 13.15 Time is of the essence in this Agreement and, without limitation, will remain of the essence after any modification or extension of this Agreement, whether or not expressly restated in the document effecting the modification or extension.

### Conflicts among provisions

- 13.16 Conflicts among provisions of this Agreement will be resolved as follows:
- (a) a provision in the body of this Agreement will prevail over any conflicting provision in, attached to or incorporated by reference into a schedule, unless that conflicting provision expressly states otherwise; and
  - (b) a provision in a schedule will prevail over any conflicting provision in a document attached to, or incorporated by reference into a schedule, unless the schedule expressly states otherwise.

### Agreement not permit nor fetter

- 13.17 This Agreement does not operate as a permit, license, approval or other statutory authority which the Contractor may be required to obtain from the Regulator or any of its agencies in order to provide the Services. Nothing in this Agreement is to be construed as interfering with, or fettering in any manner, the exercise by the Regulator or its agencies of any statutory, prerogative, executive or legislative power or duty.

### Remainder not affected by invalidity

- 13.18 If any provision of this Agreement or the application of it to any person or circumstance is invalid or unenforceable to any extent, the remainder of this Agreement and the application of such provision to any other person or circumstance will not be affected or impaired and will be valid and enforceable to the extent permitted by law.

### Further assurances

- 13.19 Each party must perform the acts, execute and deliver the writings, and give the assurances as may be reasonably necessary to give full effect to this Agreement.

### Additional terms

- 13.20 Any additional terms set out in the attached Schedule F apply to this Agreement.

### Governing law

- 13.21 This Agreement is governed by, and is to be interpreted and construed in accordance with, the laws applicable in British Columbia.

## 14 INTERPRETATION

### In this Agreement:

- (a) "includes" and "including" are not intended to be limiting;
- (b) unless the context otherwise requires, references to sections by number are to sections of this Agreement;
- (c) the Contractor and the Regulator are referred to as "the parties" and each of them as a "party";
- (d) "attached" means attached to this Agreement when used in relation to a schedule;
- (e) unless otherwise specified, a reference to a statute by name means the statute of British Columbia by that name, as amended or replaced from time to time;
- (f) the headings have been inserted for convenience of reference only and are not intended to describe, enlarge or restrict the scope or meaning of this Agreement or any provision of it;
- (g) "person" includes an individual, partnership, corporation or legal entity of any nature; and
- (h) unless the context otherwise requires, words expressed in the singular include the plural and vice versa.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): DM



This Schedule forms part of the agreement.

**Contract No: 21424001**

**DESCRIPTION OF SERVICES**

The Contractor will provide operational support on an as-needed basis to support BCER's SharePoint Online portals and related M365 infrastructure. The Gravity Union Project Manager will triage support requests and delegate tasks accordingly to appropriate personnel (Analyst, Architect, Developer) assigned to the project.

**TERM**

The term of this Agreement commences on May 1, 2023 and ends on March 31, 2024. The Regulator may, in its sole discretion, renew this Agreement for up to two, one year terms.

**INVOICES**

All invoices to the Regulator will be sent to the following:

- [Katie.Cook@bc-er.ca](mailto:Katie.Cook@bc-er.ca)
- [Derek.Mathews@bc-er.ca](mailto:Derek.Mathews@bc-er.ca)

**KEY PERSONNEL**

All notice to the Regulator will be sent to the Contract Manager:

Derek Mathews  
**Director, Architecture & Innovation**  
[Derek.Mathews@bc-er.ca](mailto:Derek.Mathews@bc-er.ca)

The Key Personnel of the Contractor are as follows:

- (a) Michael Schweitzer, Account Manager
- (b) Thabata Granja, Project Manager

Contractor Initials: MS

Oil and Gas Commission (authorized initials): DM

This Schedule forms part of the agreement.

**Contract No: 21424001**

1. Fees will be paid at hourly rates as listed below, for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, \$50,000, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Activity and Role	Cost
General Microsoft 365 and SharePoint Online support services from a Digital Transformation Analyst	\$175 per hour
General Microsoft 365 and SharePoint Online support services from a Solution and Infrastructure Architect	\$200 per hour
Project Management services	\$200 per hour

2. The Contractor should submit to the Regulator, monthly, a written statement of account showing the calculation of all fees and expenses claimed for the period for which the statement is submitted, with hours and dates.
3. After receipt by the Regulator of any aforesaid written statement of account, the fees referred to in paragraph 1 of this schedule will be paid to the Contractor by electronic funds transfer, subject always to the respective maximum amount set forth in paragraph 4 of this schedule.
4. The maximum amount payable under the terms of this Contract (the "Maximum Amount") is \$50,000, plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): DM

This Schedule forms part of the agreement.

Contract No: 21424001

**Insurance:**

1. The Contractor must, without limiting the Contractor's obligations or liabilities and at the Contractor's own expense, purchase and maintain throughout the Term the following insurances with insurers licensed in Canada in forms and amounts acceptable to the Regulator:
  - (a) Commercial General Liability in an amount not less than **\$2,000,000** inclusive per occurrence against bodily injury, personal injury and property damage and including liability assumed under this Agreement and this insurance must
    - (i) include the Regulator as an additional insured,
    - (ii) be endorsed to provide the Regulator with 30 days advance written notice of cancellation or material change, and
    - (iii) include a cross liability clause;
2. All insurance described in section 1 of this Schedule must:
  - (a) be primary; and
  - (b) not require the sharing of any loss by any insurer of the Regulator.
3. The Contractor must provide the Regulator with evidence of all required insurance as follows:
  - (a) within 10 Business Days of commencement of the Services, the Contractor must provide to the Regulator evidence of all required insurance in the form of a completed Certificate of Insurance;
  - (b) if any required insurance policy expires before the end of the Term, the Contractor must provide to the Regulator within 10 Business Days of the policy's expiration, evidence of a new or renewal policy meeting the requirements of the expired insurance in the form of a completed Regulator of British Columbia Certificate of Insurance; and
  - (c) despite paragraph (a) or (b) above, if requested by the Regulator at any time, the Contractor must provide to the Regulator certified copies of the required insurance policies.
4. The Contractor must obtain, maintain and pay for any additional insurance which the Contractor is required by law to carry, or which the Contractor considers necessary to cover risks not otherwise covered by insurance specified in this Schedule in the Contractor's sole discretion.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): DM

This Schedule forms part of the agreement.

**Contract No: 21424001**

**Definitions**

1. In this Schedule,
  - (a) "**Act**" means the *Freedom of Information and Protection of Privacy Act* (British Columbia), as amended from time to time;
  - (b) "**contact information**" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
  - (c) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Regulator and the Contractor dealing with the same subject matter as the Agreement.

**Purpose**

2. The purpose of this Schedule is to:
  - (a) enable the Regulator to comply with its statutory obligations under the Act with respect to personal information; and
  - (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

**Collection of personal information**

3. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
  - (a) the purpose for collecting it;
  - (b) the legal authority for collecting it; and
  - (c) the title, business address and business telephone number of the person designated by the Regulator to answer questions about the Contractor's collection of personal information.

**Accuracy of personal information**

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Regulator to make a decision that directly affects the individual the information is about.

**Requests for access to personal information**

7. If the Contractor receives a request for access to personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator unless the Agreement expressly requires the Contractor to provide such access and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

**Correction of personal information**

8. Within 5 business days of receiving a written direction from the Regulator to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
9. When issuing a written direction under section 8, the Regulator must advise the Contractor of the date the correction request to which the direction relates was received by the Regulator in order that the Contractor may comply with section 10.
10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Regulator, the Contractor disclosed the information being corrected or annotated.
11. If the Contractor receives a request for correction of personal information from a person other than the Regulator, the Contractor must promptly advise the person to make the request to the Regulator and, if the Regulator has advised the Contractor of the name or title and contact information of an official of the Regulator to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

**Protection of personal information**

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Contractor Initials: MS Oil and Gas Commission (authorized initials): DM

This Schedule forms part of the agreement.

**Contract No: 21424001**

**Storage and access to personal information**

13. Unless the Regulator otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

**Retention of personal information**

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Regulator in writing to dispose of it or deliver it as specified in the direction.

**Use of personal information**

15. Unless the Regulator otherwise directs in writing, the Contractor may only use personal information if that use is:  
(a) for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement; and  
(b) in accordance with section 13.

**Disclosure of personal information**

16. Unless the Regulator otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Regulator if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
17. Unless the Agreement otherwise specifies or the Regulator otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

**Inspection of personal information**

18. In addition to any other rights of inspection the Regulator may have under the Agreement or under statute, the Regulator may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

**Compliance with the Act and directions**

19. The Contractor must in relation to personal information comply with:  
(a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and  
(b) any direction given by the Regulator under this Schedule.
20. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

**Notice of non-compliance**

21. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Regulator of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

**Termination of Agreement**

22. In addition to any other rights of termination which the Regulator may have under the Agreement or otherwise at law, the Regulator may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

**Interpretation**

23. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
24. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
25. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
26. If a provision of the Agreement (including any direction given by the Regulator under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
27. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or the law of any jurisdiction outside Canada.

Contractor Initials: MS

Oil and Gas Commission (authorized initials): DM



CONTRACT No. 21424001

**CONTRACT AMENDMENT #1**

**THIS AMENDMENT MADE THIS 26<sup>th</sup> DAY OF APRIL 2024**

**BETWEEN:**

**BC ENERGY REGULATOR (HEREIN CALLED THE "REGULATOR")  
OF THE FIRST PART**

**AND:**

**GRAVITY UNION SOLUTIONS LIMITED (HEREIN CALLED THE "CONTRACTOR")  
OF THE SECOND PART**

**WITNESSETH THAT WHEREAS:**

- A. The parties hereto entered into an Information Technology Professional Services Agreement identified as Contract No. 21424001 for a term which commenced on May 1, 2023, and was scheduled to end on March 31, 2024;
- B. **AND WHEREAS** the parties have agreed to modify the Agreement.

**NOW THEREFORE IN CONSIDERATION OF THE COVENANTS AND AGREEMENTS HEREIN CONTAINED, THE PARTIES AGREE AS FOLLOWS:**

- 1. This amendment is made effective April 1, 2024.
- 2. The term of the Agreement is extended to March 31, 2025. The term described in Schedule "A" is deleted and replaced with:

The term of this Agreement commences on May 1, 2023, and ends on March 31, 2025. The Regulator may, in its sole discretion, renew this Agreement for one additional one-year term.

- 3. Maximum Fees will increase by \$35,000 from \$50,000 to \$85,000. Clauses 1 and 4 will be removed and replaced with the following:
  - 1. Fees will be paid at hourly rates as outlined below for the term during which the contractor is engaged in the fulfillment of their obligations under this Contract, including any extensions to the original term of the Contract, in no event will the fees payable to the contractor in accordance with this paragraph exceed, in aggregate, **\$85,000**, (exclusive of any applicable taxes described in section 3.1(c) of this agreement).

Activity and Role	Cost
General Microsoft 365 and SharePoint Online support services from a Digital Transformation Analyst	\$175 per hour
General Microsoft 365 and SharePoint Online support services from a Solution and Infrastructure Architect	\$200 per hour
Project Management services	\$200 per hour




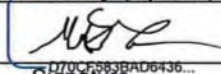
**CONTRACT No. 21424001**

**CONTRACT AMENDMENT #1**

4. The maximum amount payable under the terms of this Contract (the "Maximum Amount) is **\$85,000** plus any applicable taxes which may be incurred. There is no guarantee that the Contract Maximum Amount will be reached or that the spending will be spread evenly throughout the Contract.

5. That in all other respects, the terms and conditions of the said Agreement are hereby ratified and confirmed.

**IN WITNESS WHEREOF** the parties hereto have executed this Agreement the day and year first above written.

SIGNED AND DELIVERED on the <u>29<sup>th</sup></u> day of April 2024 on behalf of the BC Energy Regulator by its duly authorized representative:	SIGNED AND DELIVERED on the <u>26</u> day of April 2024 by or on behalf of the Contractor (or by its authorized signatory or signatories if the Contractor is a corporation).
	
Signature	Signature
<b>Derek Mathews</b>	<b>Michael Schweitzer</b>
Print Name	Print Name

# Operational Support

BC Energy Regulator – Statement of Work





BC Energy Regulator — Operational Support

# Statement of Work

March 26, 2024

## Confidentiality and Warranty

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Gravity Union Solution Limited.

The opinions expressed are in good faith and while every care has been taken in preparing these documents, Gravity Union makes no representations and gives no warranties of whatever nature in respect of these documents, including and not limited to the accuracy or completeness of any information, facts and/or opinions contained therein.

## Validity

This Statement of Work shall remain valid for 60 days.



Gold Certified

Collabware Partner



Gold

Microsoft Partner



Page 1 of 6

## Table of Contents

Proposed Scope and Effort .....	3
Estimated Project Cost.....	3
Rates .....	3
Estimated Cost .....	3
Payments.....	4
Proposed Team .....	4
Assumptions.....	4
Support .....	4
Microsoft Gold Partner .....	4
Travel and Expenses .....	5
Cancellation .....	5
Change Orders .....	5
Payment .....	5
Authorization .....	6

## Proposed Scope and Effort

The British Columbia Energy Regulator would like to continue engaging with Gravity Union to provide ongoing operational support on an as-needed basis to support their SharePoint Online portals and M365 Infrastructure support. The project budget is \$50,000. The Gravity Union Project Manager will triage support requests and delegate tasks accordingly to the Analyst or Architect assigned to the project.

## Estimated Project Cost

### Rates

Gravity Union’s standard rates range between \$175 and \$250 per hour. The Digital Transformation Analyst rate is \$175 per hour, the Project Manager rate is \$200 per hour, and the Senior Solution Architect rate is \$250 per hour.

Activity and Role	Cost
General Microsoft 365 and SharePoint Online support services from a Digital Transformation Analyst	\$175 per hour
General Microsoft 365 and SharePoint Online support services from a Solution and Infrastructure Architect	\$200 per hour
Project Management services	\$200 per hour

### Estimated Cost

Gravity Union proposes a Time & Materials project budget targeting \$50,000 where BC Energy Regulator is only billed for costs incurred, using the estimated costs below as our target budget. Any cost actuals beyond this budget would require prior approval before work execution or billing.

## Payments

Invoices would be submitted at the end of each month, for hours worked during that month, due upon receipt.

## Proposed Team

- ☑ Pauline Richer, Digital Transformation Analyst
- ☑ Denis Boico, Solution and Infrastructure Architect
- ☑ Thabata Granja, Project Manager
- ☑ Michael Schweitzer, Account Manager

## Assumptions

- ☑ Gravity Union will have sufficient access to BCER's SharePoint solution.
- ☑ Requests from BCER will be sent to the Gravity Union Project Manager and triaged accordingly.

## Support

With resources across Canada, Gravity Union's standard support from 6:00am PT to 6:00 pm PT. Gravity Union can perform work outside of these hours when scheduled in advance and can negotiate support agreements for organizations beyond our regular hours on an as-needed basis.

## Microsoft Gold Partner

As a Microsoft Gold Partner, we have access to resources and support directly from Microsoft to troubleshoot problems and issues and can escalate within Microsoft for support.

## Travel and Expenses

At current, we do not anticipate any travel costs; however, travel costs and expenses will be itemized separately from hours for billing. There will be no mark-ups on travel costs and fees incurred.

## Cancellation

The BC Energy Regulator is free to cancel this arrangement at any time. All time worked up to the notification of cancellation will be billed and owed to Gravity Union by BC Energy Regulator.

## Change Orders

Proposed changes or extensions to the contracted work statement(s) must be in writing and approved by both BC Energy Regulator and Gravity Union before the commencement of work. Additional fees will be invoiced in the regular billing cycle described below.

## Payment

The BC Energy Regulator will be billed at the end of each month for hours worked with payment due upon receipt. Included with each invoice will be a breakdown of hours with descriptions.

## Authorization

By signing the below, all parties agree to enter into a contract for services as described in this document.

### BC Energy Regulator

Name (printed) Derek Mathews

Date March 28, 2024

Signature 

### Gravity Union Solutions Limited

Name (printed) Michael Schweitzer

Date \_\_\_\_\_

Signature \_\_\_\_\_

## Summary Details of Request

File Number:	Applicant Type:	Request Wording:	Date Released:
BCER2024-003	Interest Group	<p>Copies of the following:</p> <ul style="list-style-type: none"> <li>• acceptable use of technology policy instruments (where “instrument” has the same meaning as in Treasury Board Directive 1/23) and onboarding manuals.</li> <li>• file plans/lists/indexes and/or records management ontologies/thesauri.</li> <li>• public body self-assessments and audits/evaluations of records/information management.</li> <li>• policy instruments regarding records or information management.</li> <li>• copies of record retention schedules.</li> <li>• the public body’s information resources/information asset/records management plans, as applicable; and,</li> <li>• licenses, contracts, or agreements between the public body and recordkeeping system service providers or contractors.</li> </ul> <p>Date range: 1 January 2021 to 16 July 2024.</p>	Aug 26, 2024