Third Party Information Security Guidelines – Supplier Information

1.0 Introduction and Purpose

You are receiving this document as a current or potential Enbridge supplier (a "**Supplier**") that may:

- provide technology products (e.g., hardware, software) or services to Enbridge; or
- have access to Enbridge Information and Technology Assets.

During the Supplier evaluation process, and prior to providing you with access to Information and Technology Assets, Enbridge will conduct an assessment of your information security policies and practices. As part of this assessment, Enbridge will request you to provide information to enable Enbridge to assess the extent to which your information security policies and practices align with Enbridge's requirements, in the context of the products or services that you may supply or provide to Enbridge. Enbridge will use the responses internally for the purpose of qualifying Suppliers to potentially perform services or deliver goods and/or continue to provide services or goods to Enbridge. To help you prepare for the assessment, this document articulates high-level information security requirements that Enbridge will be reviewing as part of its Supplier evaluation process.

This document reflects the approach to Supplier information security adopted by Enbridge Inc. and each of its wholly owned subsidiaries and affiliates (collectively, "**Enbridge**"), and the requirements set out in the Enbridge Policies. General principles that underpin Enbridge's approach to information security include the following:

- all Suppliers will safeguard the availability, integrity and confidentiality of the Information and Technology Assets; and
- when accessing the Information and Technology Assets, Suppliers will comply with the Enbridge Policies.

Failure to comply with these principles could cause irreparable harm to Enbridge's business, operations, reputation and financial standing. In the event of a conflict between this document and the Enbridge Policies, the Enbridge Policies will govern.

Enbridge will update its this document from time to time to reflect evolving technology, threats, standards, and regulations. Please check the Enbridge website to ensure you are reading the latest version of this document located on the Suppliers page under Work with Enbridge from the main menu.

Your cooperation will be required to complete the assessment. If information security risks are identified, it is Enbridge's intent that Enbridge and its Suppliers will communicate openly and work collaboratively to assess the risks and implement appropriate mitigations. This process will be beneficial for both your organization and Enbridge, and we hope that it strengthens relationships with our Suppliers.

If Enbridge enters into a contractual relationship with you, Enbridge will re-perform the assessment from time to time to ensure that Supplier maintains appropriate security controls and information security risks are mitigated.

2.0 Definitions

Audit
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Business Owner
A designated individual, often embedded within the business, who has overall accountability for the process or application system.

Confidential Information
Information that is intended by the Information Owner for a specific, identified audience. This information is for use solely within Enbridge or by its designated partners and is limited to those with a "need to know." The explicit approval of the Information Owner is required to release this information even to those with a need to know.

Enbridge Approved
An approval function by the Senior IT Manager, IT Director or Business Owner responsible for the delivery of a service or function.

Enbridge Policies
Enbridge's policies of general application, and its information security policies, standards, controls, guidelines and procedures including:
(i) Enbridge's Acceptable Use of Technology Assets Policy;
(ii) Enbridge's Statement on Business Conduct;
(iii) Enbridge's Lifesaving Rules; and
(iv) Enbridge's Supplier Code of Conduct.

Information Asset
Any Enbridge data in any form, and the equipment used to manage, process, or store Enbridge data, used in the course of executing business. This includes, but is not limited to, corporate, customer and partner data. Information Assets can exist in many forms: printed or written on paper, stored electronically, transmitted by post or electronically, shown on films, or spoken in conversation. This includes, but is not limited to, corporate, customer, and partner data.

Information and Technology Assets
Information or Technology Assets, or both Information and Technology Assets, as applicable.

Information Owner
The person responsible for ensuring a specific information asset is handled and managed appropriately.

Security Incident
An attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy.

Subcontractor
A third party to which Supplier subcontracts provision of all or part of the delivery of the services or provision of the products.

Supplier
A vendor, supplier or service provider that Enbridge contracts with for the procurement, management and disposition of products and/or services.

Technology Asset
An Enbridge technology asset, including:

- IT services — email, Internet and printing, software as a service, cloud services, etc.;
- IT systems — includes computers, networks, field devices, personal mobile devices, servers, data storage devices and software; and
- Industrial Control Systems – PLCs, SCADA, etc.

3.0 Information Security Requirements

3.1 Overview

To support effective onboarding of Suppliers and to protect the confidentiality, integrity and availability of Enbridge Information and Technology Assets, the information security practices and procedures of Suppliers that wish to do business with Enbridge will address the following requirements:

[Refer to the table below for a summary of which requirements apply based on how you access Enbridge Information and Technology Assets]

Type of Access	**Suppliers that have access to Enbridge Information and Technology Assets using Enbridge-managed or provided Technology Assets (e.g. laptops)**	**Suppliers that have access to Enbridge Technology and/or Information Assets using their own assets**	**Suppliers that use other organizations to provide services to Enbridge**
Applicable Requirements	Section 3.2	Sections 3.2 and 3.3	Sections 3.2, 3.3 and 3.4

3.2 Suppliers that Access Enbridge Information and Technology Assets

Cybersecurity Program Management

3.2.1 Supplier should maintain and update as necessary a comprehensive documented information security program that:

(i) contains appropriate administrative, technical, and physical safeguards to protect Enbridge Information and Technology Assets (including the definition of information security roles and responsibilities);
(ii) complies with laws and regulations;
(iii) is reviewed and revised for adequacy and effectiveness at regular intervals (at least annually, and whenever there is a material change in Supplier's practices that may materially affect the security of Enbridge Information and Technology Assets).

3.2.2 Supplier should not alter or modify its information security program, or the application of security controls, in any way that will weaken or compromise the confidentiality, availability, or integrity of Enbridge Information and Technology Assets without the express approval of Enbridge.

3.2.3 Supplier should designate a qualified individual responsible for overseeing and implementing the Supplier's cybersecurity program and enforcing its cybersecurity policy.

Cybersecurity Risk Management

3.2.4 Supplier should have a formal cybersecurity risk management program implemented which is reviewed and updated periodically (no less frequently than on an annual basis) and communicated to relevant stakeholders.

3.2.5 Supplier should identify, review, prioritize and document cybersecurity risks. Risk treatment plans should be in place for risks that are not acceptable. Accepted risks should be reviewed and updated no less frequently than annually.

3.2.6 Supplier should conduct risk assessments as necessary to address changes to the Supplier's information systems that manage process or store Enbridge Information Assets or that access Enbridge Technology Assets, and to respond to technological developments and evolving threats. Risk assessments should include the following:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Supplier;
(2) criteria for the assessment of the confidentiality, integrity, and availability of the Supplier's technology and information assets, including the adequacy of existing controls in the context of identified risks; and
(3) requirements describing how identified risks will be mitigated or accepted and how the cybersecurity program will address, track and review accepted risks.

Cybersecurity Intelligence

3.2.7 Supplier should have a cybersecurity threat intelligence program in place to ensure relevant industry and sector relevant cyber threats are gathered, analyzed, communicated and dealt with appropriately.

Human Resource Security

3.2.8 Supplier should conduct a mutually agreed upon security background check (including, where appropriate, criminal background check) for every employee with access to Enbridge's Information and Technology Assets.

3.2.9 Supplier should use codes of conduct, ethics policies or confidentiality agreements to ensure employee awareness of Supplier's information security policies and procedures, before providing access to Enbridge Information and Technology Assets.

3.2.10 Supplier should obtain written acceptance from its employees for the below training requirements, and should maintain employee training completion reports and make such completion reports available to Enbridge upon request:

(v) its codes of conduct, ethics policies, or confidentiality agreements;
(vi) its information security program; and
(vii) Enbridge Policies.

3.2.11 Supplier should review the contents of its cybersecurity awareness and training program to ensure it is updated (no less frequently than annually) and reflects current, relevant security information.

3.3 Suppliers that have access to Enbridge Information and Technology Assets using their own assets

The additional requirements set out in this Section 3.3 apply to Suppliers that have access to Enbridge Information and Technology Assets using their own technology assets.
Note these Suppliers are also required to comply with the requirements set out in Section 3.2.

Asset Management

3.3.1 Supplier should have an asset management program implemented and maintain an inventory of assets that are used in the delivery of services to Enbridge (both hardware and software) that include ownership, classification and criticality of assets. The inventory should be reviewed and updated no less frequently than annually.

3.3.2 Supplier should ensure that all the Supplier personnel and personnel of its Subcontractors use only Supplier-approved devices (including cell phones and laptops) in the delivery of services to Enbridge or to access or store Information and Technology Assets. Mobile devices should be equipped with industry standard security and encryption features, which should include at a minimum remote wipe and remote shutdown capabilities.

Access Control

3.3.3 Supplier should control access to its technology assets and Enbridge Information and Technology Assets, including implementation of the following requirements:

(i) Logical access authorizations: Supplier should maintain and follow a formal access management process to limit access to Enbridge's Information and Technology Assets only to users that have been approved to perform the services.
(ii) Logical access suspensions: Supplier should immediately notify Business Owner to promptly revoke or disable the user access rights to Enbridge's Technology Assets of any Supplier personnel (including Supplier Subcontractor Personnel) that is terminated, resigns or retires, or is reassigned from work requiring access to Enbridge's Technology Assets.
(iii) Remote access: Supplier should use Enbridge Approved methods for remote access (such as virtual private networks, secure gateways and multi-factor authentication) to systems that access or store Enbridge Information Assets.
(iv) Privileged access: Supplier should minimize administrative privileges to Information and Technology Assets. Privileged access will be granted based on principle of "least privilege", only to individuals that require such access to perform assigned job duties and limited to the minimum number of staff necessary. Privileged access accounts should be enabled only when needed and disabled immediately when not required. Privileged access should be logged, and logs should be reviewed at a defined frequency (but no less frequently than annually).

3.3.4 Supplier should ensure password controls meet the following requirements including:

(i) Encrypting passwords using "hashing" and "salting" techniques, in transit and at rest;
(ii) Enforcing password complexity requirements on users;
(iii) Limiting failed attempts before lockout;

(iv) Prohibiting obvious or common passwords; and
(v) Not sending credentials through email for password resets.

3.3.5 Supplier should review users' access rights to Enbridge Information and Technology Assets at a defined frequency (but no less than annually) following a formal review process.

Physical & Environmental Security

3.3.6 Supplier should have a policy, standard and/or procedure for physical security that applies to both employees and Subcontractors. Supplier should take appropriate steps to prevent unauthorized physical access, as well as accidental and intentional damage, to Supplier's electronic systems that access, use, store or otherwise process Enbridge's Information and Technology Assets and the physical premises that house those systems.

3.3.7 Supplier should implement environmental controls to protect the facility, technology assets and business operation against environmental risks (e.g. fire, flooding).

Network and Communication Management

3.3.8 Network security - IDS/IPS use: Supplier should subject all network traffic to electronic review and monitoring. Supplier should use Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) systems that generate alerts containing information to detect and evaluate a potential incident. Supplier should ensure that IDS/IPS have the latest signatures applied to effectively monitor for the most recent threats and vulnerabilities.

3.3.9 Network security - firewalls: Supplier should segregate its connected networks and electronic systems to ensure systems and applications are protected from outside threats. This should include utilizing industry standard firewalls to segment and protect Supplier's internal network from the Internet, and to segregate systems that access, use, or store Enbridge Information Assets from other less restricted internal networks and systems. Supplier should disable, on public-facing firewalls, all ports and services that are not required for documented business purposes.

3.3.10 Malware protection: Supplier should use anti-malware software on networks, servers, workstations and portable devices that may be used to access Enbridge's Technology Assets, or to access, use, or store, Enbridge Information Assets; the malware signatures should be regularly updated in a timely manner.

3.3.11 Unapproved wireless networks: Supplier should have all wireless network connections and devices adequately tracked, managed, authorized, and controlled to protect against threats and to maintain security for the systems and applications using the network.

3.3.12 Wireless networks encryption: Supplier should implement processes and tools to control the use of wireless local area networks, access points and wireless systems, including approved encryption methods for authorized wireless access points.

3.3.13 When required, Supplier should only use Enbridge Approved cryptographic methods as defined in the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules.

Development or Enhancement of Technology Assets

3.3.14 Supplier should have a formal change control process to guide changes affecting Enbridge's Information and Technology Assets. Changes should be approved, reviewed and tested to ensure there is no adverse impact on organizational operations and security.

3.3.15 Supplier should provide all developers application security training.

3.3.16 Supplier should have documented information security requirements defined and adhered to for new application system development and enhancement. The document should specify the requirement for security controls at different stages of the software development lifecycle including but not limited to:

(i) Functional and security testing
(ii) Vulnerability assessment
(iii) Developers access restricted to non-production environments
(iv) Security control settings implemented
(v) Risk assessment process
(vi) Documented security requirements
(vii) Secure coding guidelines and checklists
(viii) Secure design/architecture review
(ix) Source code review

Security Operations

3.3.17 Patch and updates: Supplier should follow industry best practices for patching and updating software and firmware on networks, servers, workstations and portable devices that may be used to access Enbridge's Technology Assets, or to transmit, access, use, or store, Enbridge Information Assets.

3.3.18 Log monitoring and retention: Supplier should apply appropriate monitoring and logging technologies to record relevant actions involving access to Enbridge's Information and Technology Assets, for audit, forensic, and law enforcement purposes. Supplier will maintain and review audit logs for anomalies.

3.3.19 Supplier should regularly conduct vulnerability scans and penetration-testing on Supplier systems, applications and network devices to identify vulnerabilities. Supplier should prioritize all vulnerabilities and promptly remediate detected vulnerabilities. The Supplier should also notify Enbridge of any vulnerabilities that may impact Information or Technology Assets.

3.3.20 Supplier should have documented security hardening standards for systems including desktops, laptops, mobile devices, network devices, ICS wireless devices and servers accessing, transmitting and storing Enbridge's Information Assets.

3.3.21 Supplier should have email security controls in place for the detection and prevention of malicious messages, including domain-based authentication techniques, content filtering, user education and secure transmission of messages.

3.3.22 Supplier should implement Data Loss Prevention (DLP) controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to on systems transmitting, storing or processing Information Assets.

Cybersecurity Incident Management

3.3.23 Supplier should establish, document and distribute a formal Security Incident management plan, which includes the reporting procedure, escalation procedures, and a remediation process. Any reasonably suspected or confirmed cyber incident (events or actions that may have compromised the confidentiality, integrity, or availability of Information Assets, or are reasonably suspected of having done so) must be reported to Enbridge immediately. Notification should include the nature of the event, date and time of the event, suspected amount of information exposed, steps being taken to investigate the circumstances of the exposure and remediate, and to the extent

applicable, the suspected amount of Information Assets exposed and the nature of such Information Assets.

3.3.24 The Security Incident management plan should be periodically tested, at a minimum annually, (e.g. tabletop test) to verify the soundness of the plan. Tests should be conducted based on high risk threats to the Supplier environment (e.g. virus/worm attacks, data compromise, loss of physical assets) and be relevant to the services provided to Enbridge.

Backup and Recovery

3.3.25 Supplier should have a business continuity plan developed and maintained for applications and infrastructure used in support of the services provided to Enbridge. Supplier should review and update its business continuity plan, but not less than on an annual basis, including all required updates in response to any change in the services or delivery of the services. Supplier will ensure that all applicable Supplier Subcontractors have an appropriate (determined in the context of the portion of the services to be provided by such Supplier Subcontractor) and regularly tested business continuity plan in place.

3.3.26 Supplier should have a disaster recovery plan developed and maintained for applications and infrastructure used in support of the services provided to Enbridge. Training and awareness of the disaster recovery plan should be rolled out to all key stakeholders within the organization. The disaster recovery plan should be tested and updated regularly, and at a minimum annually, to ensure that it is up to date and effective. The disaster recovery plan should include the following:

- Documented critical business functions, applications and supporting technologies.
- Document what factors trigger a disaster, who is authorized to declare a disaster, and the communication plan, including notification to Enbridge.
- Identify alternate locations with the necessary infrastructure to support the recovery needs.
- Document the management and membership of the disaster response and recovery teams.
- Document service level, RTO’s and RPO’s.
- Document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan.
- Identify critical technology service provider dependencies and recovery support capability.

3.3.27 Supplier should ensure that systems that access, store or use Enbridge Information Assets are regularly backed up. Backups of these systems and data should be available, including in the event of a disaster and the ability to restore from such backups should be tested periodically, and no less than annually.

Information classification and information disposal and reuse

3.3.28 Supplier should have standards that includes guidelines on information classification, information handling/storage, data encryption, data retention and secure data disposal.

3.3.29 Information Assets, including any backups, should be secured through whole disk or media encryption and file or database encryption (if applicable) and strong access controls. Transmission of Information Assets must be encrypted.

3.4 Suppliers that use Subcontractors to Provide Products or Services to Enbridge

The additional requirements set out in this Section 3.4 apply to Suppliers that use subcontractors (including any fourth parties) parties in providing products or services to Enbridge.
Note: These Suppliers are also required to comply with the requirements set out in Sections 3.2 and 3.3 above, as applicable, based on how they access Enbridge Information and Technology Assets

Sub-service Provider (Fourth Party)

3.4.1 Supplier must assess and track cybersecurity and information security risk associated with Subcontractors or its service providers with access to Enbridge's Information and Technology Assets and should take all commercially reasonable actions to promptly remediate these risks.

3.4.2 Supplier must contractually obligate Subcontractors or its service providers to protect Enbridge Information and Technology Assets when accessed, processed, or stored by a Subcontractor or service provider, to the same level required of the Supplier.

3.4.3 A Supplier storing sensitive Enbridge Information Assets must demonstrate compliance with information security and confidentiality, service definitions, and service level agreements and must undergo Audit and review (e.g. SOC 2 Type II assessment, ISO 27001, or industry recognized information security audit, assessment or certification of similar rigor) conducted by a qualified independent third party, and at planned intervals to govern and maintain compliance with the service delivery agreements. Results of the assessment, Audit or certification must be made available to Enbridge on an annual basis.