Enbridge Inc. Cybersecurity Policy

Public Summary

ENBRIDGE®

May 2026

Enbridge Cybersecurity Policy

Public Summary

Purpose

Protecting Enbridge's technology assets through a risk-based approach supports safe, reliable, and secure operations. As a result, protecting confidentiality, integrity, availability, and reliability of information and services is important to our business. The purpose of Enbridge's Cybersecurity Policy is to set out executive leadership's approach to managing cybersecurity risk and protecting assets from a wide range of threats.

Scope

This Enbridge Cybersecurity Policy (the "Policy") applies to and has been adopted by Enbridge Inc. and each of its wholly owned subsidiaries and affiliates. This Policy applies to all Enbridge employees, directors, contractors, and agents of Enbridge (collectively, "Users") and covers both information technology (IT) and operational technology (OT) cybersecurity. This public summary does not describe internal enforcement processes, which are addressed in Enbridge's internal policy framework.

Regulatory and industry standards alignment

The Policy and cybersecurity program are informed by recognized industry standards, frameworks, best practices, and regulatory guidance applicable to the energy and critical infrastructure sectors, where Enbridge operates. Examples include:

- Transportation Security Administration (TSA) Pipeline Security Guidelines and Security Directives
- 33 CFR Parts 101.600 to .670 (United States Coast Guard cybersecurity regulations)
- North American Electric Reliability Corporation (NERC) Reliability Standards – Critical Infrastructure Protection (CIP)
- CSA Standard Z246.1 – Security Management for Petroleum and Natural Gas Industry Systems
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- ISO/IEC 27000 series information security standards

These references help guide how Enbridge identifies, assesses, and manages cyber risks, while enabling continuous improvement as threats, technologies, and regulatory expectations evolve.

Risk management, strategy and governance

Oversight of cybersecurity is integrated into the responsibilities of the Enbridge Inc. Board of Directors (Board) and its committees, with primary oversight residing with the Audit, Finance and Risk Committee. Enbridge's management is responsible for implementing risk management strategies and monitoring performance. The technology and information services function is centralized under the Senior Vice President & Chief Information Officer (CIO). Reporting to the CIO, is the Chief Information Security Officer, who oversees the cybersecurity program. This Policy is one part of a broader framework of policies, standards, controls, and related requirements, including the Acceptable Use of Technology Assets Policy, Artificial Intelligence Policy, and other cybersecurity standards.

Policy

The Policy is designed to support the following commitments:

Cybersecurity organization

Enbridge establishes and maintains organizational roles to manage cybersecurity at Enbridge.

Assurance and continuous improvement

Enbridge maintains a risk-based cybersecurity assurance program intended to evaluate the ongoing effectiveness of its cybersecurity controls and to support continuous improvement. The program is reviewed periodically to reflect emerging threats, evolving technology, and changes in the regulatory landscape. Enbridge conducts assessments of its cybersecurity standards, tests its ability to respond to and recover from incidents, and monitors the environment for potential threats.

Protection of Enbridge Assets

Enbridge uses appropriate measures intended to secure and safeguard information assets and technology systems ("Assets") to preserve data integrity, confidentiality, and availability throughout their lifecycle.

- Enbridge maintains processes to identify and manage Assets in a manner appropriate to their risk and function
- Assets are subject to cybersecurity measures that reflect their importance and value to the organization
- Operational controls are employed to integrate cybersecurity considerations into operational management of the Assets
- Enbridge uses controls intended to help manage the risk of unauthorized physical access, damage, theft, interference, or compromise of Assets
- Enbridge uses controls intended to reduce the risk of loss or damage and to support recovery of information resources in line with the business objectives
- Information being transmitted and transferred within Enbridge and/or to any external entities are subject to levels of security measures appropriate to the nature of the information and relevant risk
- Cybersecurity considerations are incorporated into the development, implementation, enhancement, and maintenance of Assets
- Enbridge establishes cybersecurity expectations for third parties regarding Assets accessible to or maintained by third parties, including compliance with Enbridge's standards and contractual obligations
- Enbridge workstations, mobile devices, and connected devices are subject to security management measures intended to support authorized and compliant use
- Access decisions are guided by principles such as "least privilege" and "need to know", as appropriate
- Data or information disposal and reuse practices are intended to adhere to internal records management requirements

Threat monitoring and incident response

Enbridge monitors cybersecurity threats and events and maintains processes to identify, assess, respond to, and recover from cybersecurity incidents in a safe and coordinated manner.

Individual responsibility and awareness

Cybersecurity is a shared responsibility. All personnel are expected to act in accordance with this Policy and to complete required security awareness and training activities.

Third party and supply chain security

Enbridge establishes security expectations for third parties, suppliers, and service providers that access Enbridge systems or information, consistent with a risk based approach.

Compliance and reporting

This policy and Enbridge's overall cybersecurity program are intended to support compliance with applicable laws, regulations, and contractual obligations. Personnel are expected to report suspected cybersecurity incidents or security concerns through established internal reporting channels.

Document control

This public summary reflects Enbridge's enterprise cybersecurity governance approach and high-level program principles. Detailed cybersecurity policy, standards, procedures, and technical controls are maintained internally and reviewed on a regular basis.