INFORMATION SECURITY POLICY

Approved by: President & CEO
Effective: July 27, 2020

1.0 Objective

The Information Security Policy (the "Policy") provides a security framework aimed at protecting the data, IT infrastructure, and information systems of Canadian Pacific Railway Limited ("CPRL") and Canadian Pacific Railway Company ("CPRC") and their respective subsidiaries (collectively, "CP") from unauthorized access, loss or damage, and ensures compliance with applicable regulatory requirements. The Policy provides management direction and support to establish sound business and operational practices that minimize information security risks and impacts. The Policy also informs the establishment of appropriate directives, standards, guidelines, and procedures which may be developed and published separately.

2.0 Policy Statement

CP is dedicated to securing its data, IT infrastructure, and information systems, which are vital to CP's mission and objectives, by taking appropriate measures to preserve the confidentiality, integrity, and availability of its systems and information. CP understands that information security risks can have a significant impact on its business operations, customer relationships and reputation in the marketplace and recognizes the need to develop and apply appropriate measures to manage these risks. By maintaining a robust set of information security practices, CP strives to protect its operations by providing secure, efficient, and reliable transportation solutions for customers.

3.0 Scope

The Policy applies to all CP information assets, supporting systems, and personnel including employees, directors, officers, agents, contractors and representatives (collectively, "CP Personnel") who access CP's information assets and systems. With respect to CP Personnel who perform services for CP and who are not in a direct employment relationship with CP, to the extent applicable, it is expected that such CP Personnel will either abide by the Policy or undertake, as a condition of their engagement with CP, to adhere to the principles and standards of business conduct consistent with the Policy.

4.0 Commitments

The following information security commitments define how CP will ensure consistent application of secure procedures across CP's operations. These information security commitments support CP's objectives to protect its data, information systems, IT infrastructure, and operations at all levels, and ensure compliance with regulatory

History

Version	Date
1	July 27, 2020

requirements by implementing best practices for information security standards, procedures, and guidelines.

In accordance with the Policy, CP is committed to:

- Protecting its data, IT infrastructure and information systems throughout CP's operations by addressing known cyber threats, including unauthorized access to CP's data and systems, disclosure of CP's confidential information, trade secrets, intellectual property assets, or other inappropriate use that may lead to or cause disruption to CP operations, or jeopardize CP interests or image;
- Maintaining an information security management system to provide consistent and effective guidance and resources to CP employees in line with industry best practices and relevant elements of ISO 27001 and the NIST Cybersecurity Framework;
- Managing internal security procedures and implementing an escalation process that employees must follow in case of a suspicious event;
- Monitoring and regularly reporting on CP's information security performance across the company and CP's operations;
- Maintaining an information security auditing program that monitors compliance with the Policy;
- Continuous monitoring of networks, information systems and IT infrastructure for potential security breaches or threats, and establishing contingency plans and incident response procedures. CP information assets and systems may be monitored at any time without prior notice in accordance with applicable laws and regulations;
- To the extent possible, and where cost effective, CP will automate the enforcement of the Policy and related procedures.

5.0 Implementation

- Implementation of the Policy is led by the Chief Information Officer and the Senior Director for Enterprise Security.
- Full implementation of all commitments and appropriate monitoring and reporting requires a period of transition. CP will review procedures, communication and training needs and other documents or processes to provide for alignment, consistency and effective governance of the Policy. Accordingly, the current projected completion date for implementation of the Policy will be July 29, 2022.
- All CP Personnel are expected to comply with the Policy in the context of their work for CP. Any non-compliance with the Policy may result in a disciplinary action, up to and including termination of employment, or legal action as appropriate, or both.

History

Version	Date
1	July 27, 2020

- As part of the on-boarding process, it is mandatory for new employees to review the Policy. All employees are provided relevant security training on a regular basis. Training is updated periodically to stay current with changes to the industry, regulatory requirements and relevant threats.

- CP's Personnel and the public can report known or suspected issues of non-compliance with the Policy directly to their manager or by using CP's confidential, anonymous and independently managed Alert Line (A-Line) at 1-888-279-6235 or filing a report at https://secure.ethicspoint.com/domain/media/en/gui/22547/index.html

History

Version	Date
1	July 27, 2020