VIA Rail Canada Standard

Third Party

In support of the Corporate Information Security Policy (CISP)

Standard owner: Patrick Patenaude **Effective date:** Monday, August 22, 2022

1 OBJECTIVE

This Standard articulates the information security requirements that a Third Party shall respect to protect VIA Rail's Information and IT Assets. All VIA Rail's Third Parties shall manage VIA Rail's High Protection information assets (HP assets) to safeguard its availability, integrity, and sensitivity.

Some Third Parties may be provided access to VIA Rail's IT Assets, and consequently VIA Rail's Information Assets, and in doing so shall respect VIA Rail's corporate Policies and Standards to maintain the level of protection on VIA Rail's IT Assets and prevent cyber-attacks on VIA Rail's Information and IT Assets which could cause irreparable harm to VIA Rail's business, operations, reputation and financial standing.

2 SCOPE

This Standard applies to all Third Parties who are providing VIA Rail with Information Technology services, Operational Technology services or services whereby they host, store or access VIA Rail's High Protection assets. Additionally, when accessing VIA Rail's IT Assets, they shall comply with VIA Rail's Corporate Information Security Policy, Directives, Standard and Security matrixes.

Third Parties are also expected to comply with the Information Security provisions set forth in VIA Rail's Code of Ethics to safeguard the availability, integrity and sensitivity of VIA Rail's IT Assets and its High Protection assets.

Compliance Criteria

Deviations of the controls set forth in this document shall be communicated to VIA Rail. Please forward requests to Cybersecurity_Team@viarail.ca.

3 DEFINITIONS

High Protection (HP)

assets that contain protected information such as critical infrastructure information, sensitive security information and any information that is sensitive by its nature, whether it is marked VIA-Personal Information or VIA-Restricted, that is communicated by VIA Rail to a Third Party and that VIA Rail desires for a Third Party to keep sensitive and use only for the purpose of its relationship with VIA Rail

Examples of HP Assets

- VIA Rail's commercially or competitively sensitive, proprietary or private information including information of a business, commercial, industrial, scientific, strategic, or technical nature
- All data that is classified as VIA-Internal, VIA-Restricted and VIA-Personal Information
- Personal Information (as defined in the Privacy Act) handled by VIA Rail
- VIA Rail Intellectual Property
- formulas, processes and mechanisms
- data, plans, drawings, operational, technical, commercial, financial or investment plans
- business and strategic operating plans
- new product, brand and marketing strategies, plans and forecasts, strategic alliances, development of new products and business areas
- customer lists and contact information, needs, purchasing history, rates, specifications and preferences
- contracts and agreements
- legal information including that covered by legal privilege
- corporate transactions, mergers and acquisitions
- competitive intelligence and market information compiled for VIA Rail
- internal communications, memoranda, presentations
- supplier lists
- information about VIA Rail's IT systems, infrastructure and operations
- corporate data

Information Assets	All of the data or databanks, information systems, or media, printed documents, forms, information technology installations, or any combination thereof, and including operational technologies that are the property of VIA Rail;
Personnel	means Third Party's employees, agents, consultants, subcontractors or representatives, if any, involved in the supply of services
Third Party	means suppliers, governments, non-governmental organizations or any other entities (including their personnel) with whom VIA Rail has a relationship and may share its HP assets with.
Operational technologies	(or "OT"), Thehardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc.Such technologies include SCADA systems.
VIA Rail IT Assets	means the information technology assets, operational technologies and environments, networks, equipment, computers, systems, devices, servers, applications, software, facilities and infrastructure.

4 ROLES AND RESPONSIBILITIES

Third Parties shall be aware of VIA Data Classification. They shall implement the necessary controls as defined in VIAs Standards and Matrixes.

Information Assets are identified, classified, and assigned to specific Data Owners. Adequate rules and regulations of their use are established and enforced.

The purpose is to establish a framework for classifying and defining appropriate handling and security controls to be applied on VIA Rail Information Assets. The classification level is based on its level of sensitivity, value and Criticality to VIA Rail.

All VIA Rail Information Assets shall be classified into one of four (4) levels upon creation, or after the creation or acceptance of ownership by the Data Owner.

5 Standard

There are four defined classifications used at VIA. The four levels are:

- **VIA-Public:** Data that is generally publicly available and intended for public use. This information may be freely distributed to all VIA Rail's employees, consultants and third parties as there is no concern of unauthorized disclosure. Access controls are necessary to protect data integrity.

- **VIA-Internal**: Data that is not generally available to the public or to parties outside of VIA Rail Personnel. The risk of disclosure and harm to VIA Rail are potentially low. However, little to no adverse effects on VIA Rail's operations, assets, reputation, financial position, privacy obligations shall result if exposure of this data occurs.

- **VIA-Restricted**: This data is considered information intended for restricted use (on a need-to-know basis) within VIA Rail. Access to VIA-Restricted data has a high level of risk associated with these data types and they shall be substantially protected from unintended or unauthorized disclosure, loss, or destruction, as this could have substantial and potentially costly negative effects to VIA Rail. Unauthorized exposure or loss of VIA-Restricted data could contribute to legal violations, and reputational, financial, or operational damage.

- **VIA-Personal Information**: Because it contains Personal Information, the access to VIA-Personal Information data has a high level of risk and shall be substantially protected from unintended or unauthorized disclosure, loss, or destruction, as this could have substantial and potentially costly negative effects to VIA Rail. Unauthorized exposure or loss of VIA-Personal Information data could contribute to fraud, legal violations, reputational, financial and operational damage.

The four (4) levels of Data Classification are covered by two types of protection, as specified in CISD and CISS, and in particular the Data Handling Standard:

- High Protection (or "HP" for VIA-Restricted and VIA-Personal Information)
- Normal Protection (or "NP" for VIA-Internal and VIA-Public).

Third Parties shall focus time and energy in applying standard controls (across all the Information Assets and focusing on additional controls on high-value assets (HP) for stronger protection as defined in the CISP, CISS and CISM.

Other classification levels

Some of the classification levels defined by the Canadian Government can be used within the context of VIA Rail. Documents and data received by VIA Rail and classified as such (known as Protected and Classified Information) are under strict control and accessed by a very limited number of employees based on security clearance rights and the need-to-know principle. Note that these classifications are still enforced, and their values supersede the classifications defined above. For clarification, please refer to the Corporate Security Team.

5.1 Cybersecurity Certifications, Frameworks and Standards (Applies to HP)

Third Parties shall implement a comprehensive and structured approach to protecting VIA Rail's HP assets within their IT Assets. Their approach shall include an information security program comprised of Policies, Directives, Standards. Third Party information security programs shall either be aligned with, certified by, or adopts the current versions of, one or more of the following:

- ISO/IEC 27000 series information security Standard
  - In Particular 27002:2013
- NIST Cybersecurity Framework
  - In Particular NIST CSF V1.1
  - NIST Privacy
- Cloud Security Alliance CSA STAR certification
- AICPA SOC 2 Type 2 Attestation
- ISAE 3402

5.1.1 Exposure to security risks (Applies to HP and NP)

Third Parties shall evaluate and monitor their exposure to security risks and other threats and take appropriate measures to address the associated risks to facilities, Third Party IT Assets, and VIA Rail HP assets.

5.1.2 Security Awareness (Applies to HP and NP)

Third Party shall have an ongoing Information Security Awareness program in place

5.1.3 Security Program Documentation (Applies to HP and NP)

Third Party shall document its information security program and security controls in a policy, Directive or Standard that can be made available to VIA Rail upon request.

5.2 Risk Management Programs and Methodologies (Applies to HP)

Third Parties shall adopt a comprehensive and structured approach to risk management that identifies and mitigates risks associated with their IT Assets and cybersecurity such as:

- Factor Analysis of Information Risk (FAIR)
- ISO/IEC 27005
- ISACA COBIT 5
- NIST SP 800-30
- Committee of Sponsoring Organizations (COSO)
- Information Security Forum IRAM 2

5.2.1 Exposure to cybersecurity risks (Applies to HP and NP)

Third Party shall evaluate and monitor its exposure to cybersecurity risks and other information security threats through regular review and revision and take appropriate measures to address the associated risks to Third Party IT Assets and VIA Rail's HP Assets and such reports shall be made available to VIA Rail upon request.

5.3 Security Controls (Applies to HP and NP)

Third Parties shall implement the following security controls:

- Have change control processes, including regular release management cycles
- Security patches/fixes and changes to IT Assets shall be controlled and follow change management procedures and approved operational change windows, which, where appropriate, may be agreed between VIA Rail and Third Party.
- Development, test, production and back-up environments that are physically and logically separated to reduce the risk of unauthorized access or changes to production environments.
- Controls to prevent altering any code belonging to VIA Rail without prior written permission
- Back-up and retention Standard that defines frequency of back-ups and retention cycles for all data and environments as required for the performance of their services in accordance with any agreements for such services.
- Intrusion detection, prevention, and recovery controls that protect against malicious code and maintain all anti-virus software and signatures current and actively running to detect and remove malware.
- Detection tools that prevent users from downloading programs or other material from the Internet or use of any type of removable media (including USB, CD/DVD media) on Third Party IT Assets that may store, access or process VIA Rail HP assets unless they have been authenticated as originating from a trusted source and scanned for viruses.
- Password complexity Standards to mitigate weak password threats
- Multifactor or Two-Factor authentication is active for all remote accesses including VPN access.
- Network and physical perimeter security.

5.4 Security and Operational Log Management and Access (Applies to HP and NP)

Third Party IT Assets shall be configured with log management capabilities that:

- track security and operational transactions, incidents, activities, access to information or programs, system events such as alerts, console messages and system errors, and detection, prevention, and recovery controls with respect to all aspects of the relationship with VIA Rail and services managed by Third Party.
- manage log lifecycles and are retained and available for at least fifteen months beyond the business services or relationship purpose, or longer where specified in the relevant agreement and where required by laws or regulations applicable to the services or relationship of the Third Party
- Are protected against tampering and unauthorized access (repudiation).

5.4.1 Log Availability (Applies to HP and NP)

Third Party shall make its logs available to VIA Rail either regularly or upon request for audit and archival purposes.

5.5 Audit Rights (Applies to HP)

To perform security assessments, and upon reasonable notice, Third Party shall permit VIA Rail or its partners (including government regulators requiring inspections of VIA Rail) to access VIA Rail's HP assets that are hosted, stored, accessed or otherwise processed in Third Parties IT Assets.

5.5.1 Non-Compliance Section 5.1 (Applies to HP and NP)

Where a Third-Party cannot comply or are not subjected to Section 5.1, the supplier agrees to the following as an alternative:

- Complete VIA provided Vendor Assessment Questionnaire annually.
- Co-operate with and provide all required documentation or evidence to VIA in the completion of the Vendor Assessment Questionnaire.
- Co-operate with any Third Party mandated by VIA to perform the Vendor Assessment.

5.5.2 Security Gaps (Applies to HP and NP)

Where the Third-Party Assurance or Audit demonstrates a gap with the requirements in this document, the supplier agrees to:

- Provide a plan to VIA with corrective actions within 30 calendar days.
- Obtain VIA's approval on the plan.
- Perform the corrective actions within 90 calendar days of VIA approval.
- Provide proof of completion of the corrective actions to VIA.
- Non-compliance may result in contract cancellation

5.6 Physical Access (Applies to HP and NP)

The supplier will ensure physical security. This includes:

- Physical access to any equipment that is on the premises of the Supplier's facilities and contains any information assets of VIA.
- Any mobile storage devices or any other access on the endpoints that allow employees to potentially take away data from the premises.
- Scenarios for moving and storing electronic data off-site (or hot site).

5.7 Information Access (Applies to HP and NP)

Prior to performing any services, the supplier and its employees, agents and Subcontractors who may access VIA HP assets and software shall have executed agreements concerning access protection and data/software security that are consistent with the terms and conditions of this agreement. The supplier and its employees, agents and Subcontractors shall comply with VIA Rail – Corporate Information Security Policy and all of VIA's Affiliates' policies and procedures regarding data access, privacy and security, including those prohibiting or restricting remote access to VIA Systems and VIA HP assets.

5.8 Third Party on-premises compliance with VIA Rail Standard (Applies to HP and NP)

When a Third-Party access (whether on premises or through a remote session) VIA Rail's IT Assets and HP assets; VIA Rail's Corporate Information Security Standard (CISS) and Corporate Information Security Matrix (CISM) apply and the Third Party shall respect them and any specific instructions provided by VIA Rail with respect to a specific engagement, mandate, agreement, access or statement of work. It is forbidden for Third Parties to:

- attempt to circumvent or override VIA Rail's security controls
- act in a way that constitutes a violation of criminal law
- participating in phishing or other unauthorized access or disclosure schemes
- seek or gain unauthorized access to, or attack the integrity of, VIA Rail IT Assets or attempt to do so
- willfully or recklessly spread computer viruses
- remove or tamper with security safeguards, controls or systems installed or configured by VIA Rail
- destroy, alter or encrypt VIA Rail HP assets, inadvertently or with the intent of making it inaccessible to VIA Rail
- intercept, listen in on or interfere with VIA Rail's voice, data or other electronic communications
- use VIA Rail IT Assets for any purpose other than the purpose they are intended for or the Third Party's defined mandate or services, notably it is prohibited to run a personal business or conduct business transactions unrelated to the performance of their duties for VIA Rail.

5.8.1 Information Ownership (Applies to HP and NP)

VIA Rail IT Assets that are made available to Third Parties remain VIA Rail's sole property. Third parties shall have no expectation of privacy when using VIA Rail's IT assets nor expect that anything that is stored or received on or sent from VIA Rail's IT Assets is Third Party's private property or information.

5.9 Personnel (Applies to HP and NP)

The Third Party is responsible for the acts and omissions of its personnel and as such shall for all personnel who may have access to Third Party IT Assets or have access to or custody of VIA Rail IT assets, facilities, and VIA Rail HP assets shall

- conduct background and reference checks
- manage their personnel's performance to ensure they perform in accordance with the requirements of this Standard
- provide suitable cybersecurity training and awareness programs.

5.10 Information Exchange Standard and Procedures (Applies to HP and NP)

Third Party shall use best practices for the exchange of information, for example, use secure managed file transfer services when sharing or exchanging VIA Rail HP assets with VIA Rail or any of VIA's approved collaboration tools.

5.10.1 Unauthorized Access (Applies to HP and NP)

VIA requires notification to our customers and employees when their personally identifiable information is lost or stolen. Additionally, unauthorized access or disclosure of non-public data is a breach. The supplier will provide notification within 48 hours of a breach being identified.

5.10.2 Breach Notification (Applies to HP and NP)

The supplier shall provide notification within 24 hours if a breach is suspected.

The breach shall be communicated to the VIA Advisor, Privacy & Information Management (**ATIP@viaRail.ca**) with details and be made available within 48 hours.

6 SUPPORTING DOCUMENTATION

6.1 Annexes

This Standard contains the following annexes:

None

6.2 Related Standards and Matrixes

- Data Classification Standard
- Data Classification Matrix
- Security Baseline
- Security Matrix

6.3 Resources

ISO/IEC 27002:2013 Standards
NIST CSF
FAIR
AICPA SOC 2 Type 2 Attestation

7 REFERENCES

- Code of Ethics
- Privacy Policy
- Corporate Information Security Policy
- InfoSec Charter

8 REQUESTS FOR INFORMATION

Questions regarding the interpretation of this procedure *[or* directive*]* shall be addressed to *position/office*, specifically to the attention of:

Patrick Patenaude
Senior Advisor, Governance, Risk Management & Compliance
patrick_patenaude@viaRail.ca

9 APPROVAL AND REVISION HISTORY

This Standard is to be reviewed by the Standard Owner every 2 years.

9.1 Approval

This Standard is approved and effective as of the date indicated below:

Patrick Patenaude
Sr. Advisor, Governance, risk management and Compliance
Title of Approving Authority

Monday, August 22, 2022
Date

9.2 Revision History

Version	Description of major change(s)	Effective date
3.4	*Version number aligned with the CISP*	*2020/09/14*
3.5	*Adjusted minor items. Replaced should and must with shall*	*2022/08/22*