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 Assets. All VIA Rail's Third Parties shall manage VIA Rail's information assets to safeguard their availability, integrity, and sensitivity.

Some Third Parties may be provided access to 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 Information Assets and prevent cyber-attacks on VIA Rail's Information 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 Assets or services whereby they host, store, or access VIA Rail's Information assets. Additionally, when accessing VIA Rail's Information Assets, they shall comply with VIA Rail's Corporate Information Security Policy, Directives, Standards, 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 Information Assets and its High Protection assets.

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 Information assets with.
Operational technologies	(or "OT"), The hardware and software are 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.

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 for 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 to 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 is potentially low. However, little to no adverse effects to VIA Rail's operations, assets, reputation, financial position, and 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, and 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 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 on 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 may supersede the classifications defined above. For clarification, please refer to the Corporate Security Team.

5.1 Cybersecurity Certifications, Frameworks, and Standards

Third Parties shall implement a comprehensive and structured approach to protecting VIA Rail's Information assets. Their approach shall include an information security program comprised of Policies, Directives, and 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:

- 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
- ISO/IEC 27000 series information security Standard
  - In Particular 27002:2013 may be considered appropriate.

5.2 Exposure to security risks

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

5.3 Security Awareness

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

5.4 Security Program Documentation

The 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.

5.5 Risk Management Programs and Methodologies

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)
- NIST Risk Management Framework (RMF) SP 800-37 Rev2
- ISO/IEC 27005
- ISACA COBIT 5
- Committee of Sponsoring Organizations (COSO)
- Information Security Forum IRAM 2

5.6 Security Controls

Third Parties shall implement the following security controls:

- Efficiently plan and **manage** enterprise releases, product releases, and deployment **processes**;
- A Vulnerability management process that identifies, evaluates, treats, and reports on security vulnerabilities in systems and the software that runs on them;
- Security patches/fixes and changes to Information Assets shall be controlled and follow change management procedures;
    - change management procedures and approved operational change windows, which, where appropriate, may be agreed upon between VIA Rail and Third Party;
- Development, test, production, and backup 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 the 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 Information Assets that may store access, or process VIA Rail Information assets unless they have been authenticated as originating from a trusted source and scanned for viruses;
- Password complexity Standards following NIST recommendations;
- Multifactor or Two-Factor authentication is active for all remote accesses including VPN access;
- Multifactor or Two-Factor authentication is active for all accesses to cloud services based on conditional access;
- Establish Internal, external, and perimeter information security;

5.7 Security and Operational Log Management and Access

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

- Track security and operational transactions;
- Track incidents, activities, access to information or programs, and system events such as alerts; including but limited to;
  - 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 the Third Party;
- Manage logs;
  - They must be retained and available for at least 3 months online and fifteen months offline;
  - Or for relationship purposes;
  - 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 safeguarded against tampering and unauthorized access (repudiation).

5.8 Log Availability

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

5.9 Audit Rights (Applies to HP only)

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 Information Assets.

5.10 Validation of Security Compliance

The Third-Party supplier agrees to the following:

- Where a SOC2 Type II report can be supplied, it is to be supplied annually;
- Where a SOC2 Type II report cannot be supplied;
  - Complete the 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.

5.11 Security Gaps

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 of 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.

5.12 Non-Compliance

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

5.13 Physical Access

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).

5.14 Information Access

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 – with this Standard and all VIA's Affiliates' policies and procedures regarding data access, privacy, and security, including those prohibiting or restricting remote access to VIA Systems and VIA Information assets.

5.15 Information Ownership

VIA Rail Information 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 Information assets nor expect that anything that is stored or received on or sent from VIA Rail's Information Assets is Third Party's private property or information.

5.16 Third-Party on-premises compliance with VIA Rail Standard

When Third-Party access (whether on-premises or through a remote session) VIA Rail's Information Assets;

- VIA Rail's Corporate Information Security Standard (CISS) and Corporate Information Security Matrix (CISM) shall be applied and respected including 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; including but not limited to;
  - removing or tampering with security safeguards, controls, or systems installed or configured by VIA Rail;
  - destroy, alter, or encrypt VIA Rail Information assets, inadvertently or with the intent of making them inaccessible to VIA Rail
- intercept, listen in on, or interfere with VIA Rail's voice, data, or other electronic communications;
- act in a way that constitutes a violation of criminal law; including but not limited to;
  - participating in phishing or other unauthorized access or disclosure schemes;
  - seek or gain unauthorized access to, or attack the integrity of, VIA Rail Information Assets or attempt to do so;
  - willfully or recklessly spread computer viruses;
- use VIA Rail Information Assets for any purpose other than the purpose they are intended for or the Third Party's defined mandate or services;
- It is prohibited to run a personal business or conduct business transactions unrelated to the performance of their duties defined mandate for VIA Rail.

5.17 Personnel

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 Information Assets or have access to or custody of VIA Rail Information assets, facilities shall;

- conduct background and reference checks;
- provide suitable cybersecurity training and awareness programs or participate in VIA`s Security Awareness programs;
- manage their personnel's performance to ensure they perform in accordance with the requirements of this Standard;

5.18 Information Exchange Standard and Procedures

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 Information assets with VIA Rail or use any of VIA's approved collaboration tools.

5.19 Unauthorized Access

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.

5.20 Breach Notification

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*
3.5.1	*Adjusted minor items. Updated some frameworks versions to be applied*	*2023/01/24*