November 1, 2025

Written Information Security Program

Table of Contents

8801 Trans-canada Hwy, Suite 500
Saint-Laurent, QC H4S 1Z6
514 331-4000
www.tfiintl.com

8801 Trans-canada Hwy, Suite 500
Saint-Laurent, QC H4S 1Z6
514 331-4000
www.tfiintl.com

1.0 Purpose

This Written Information Security Program ("WISP") describes the principles and governance structure through which TFI International manages cybersecurity risks, protects information assets, and supports business resilience. The WISP aligns to the NIST Cybersecurity Framework (NIST CSF) version 2.0 and reflects TFI International's commitment to safeguarding data entrusted by customers, employees, partners, and shareholders.

The WISP establishes the governance approach, risk management philosophy, and core cybersecurity capabilities that guide control expectations across TFI International and its affiliated business units. The WISP also supports compliance with applicable legal, regulatory, and contractual obligations in the jurisdictions where TFI International operates.

2.0 Scope

This program applies to all TFI International entities and affiliates, and to all systems, networks, applications, data, and cloud services used to conduct business operations. It applies to employees, contractors, service providers, and partners that handle or have access to TFI International information assets.

Information assets include confidential business information, customer data, financial information, and intellectual property, regardless of format or storage location.

The WISP is supported by internal policies, standards, procedures, and guidelines that establish detailed control requirements and implementation practices.

3.0 Cybersecurity Governance (GOVERN)

3.1 Board Oversight

Cybersecurity is governed as a core element of enterprise risk management. The Board of Directors is responsible for oversight of cybersecurity risk, including:

- Annual review of cybersecurity posture and key risks.
- Evaluation of program maturity and improvement efforts.
- Oversight of major cybersecurity initiatives.
- Review of material incidents and executive response.

The Vice President of IT Security provides an annual briefing to the Board and more frequent updates to executive leadership.

3.2 Executive Accountability

The Vice President of IT Security leads the cybersecurity risk management program and reports to the Vice President of IT, who reports to the Chief Financial Officer. Executive leadership is responsible for ensuring that cybersecurity strategies, initiatives, and investments align with business objectives and risk appetite.

8801 Trans-canada Hwy, Suite 500
Saint-Laurent, QC H4S 1Z6
514 331-4000
www.tfiintl.com

3.3 Risk Management Integration

Cybersecurity risk management is integrated into TFI's broader risk management practices, including:

- Assessment of risks to critical systems and data.
- Prioritization of mitigation activities based on business impact.
- Evaluation of supply chain risks.
- Alignment to applicable regulatory requirements.

3.4 Policy Framework

TFI maintains a central cybersecurity policy framework, including:

- Written Information Security Program.
- Cybersecurity policies and standards.
- Supporting procedures and guidelines.

Affiliates apply these policies in a risk-based manner, accounting for business context and regulatory obligations, while adhering to central expectations.

4.0 Identify (ID)

TFI identifies cybersecurity risks to systems, data, and operations through the following practices:

4.1 Asset Management

- Identification of critical systems and data types.
- Inventory of technology assets, including cloud services.
- Classification practices to guide protection efforts.

4.2 Risk Assessment

- Periodic assessments to understand threats, vulnerabilities, and potential business impact.
- Evaluation of emerging risks and technology changes.
- Prioritization of risk treatment activities based on potential impact to operations and stakeholders.

4.3 Supply Chain Risk

- Diligence of third parties with access to sensitive data.
- Contractual requirements for data security and confidentiality.
- Oversight of critical service providers.

5.0 Protect (PR)

TFI implements safeguards to protect data and reduce the likelihood and impact of cybersecurity events.

5.1 Access Control & Identity Management

- Role-based access controls.
- Multi-factor authentication for sensitive access.
- Principles of least privilege and separation of duties.

5.2 Data Security

- Encryption of sensitive data consistent with policy requirements.
- Data handling practices designed to protect confidential information.
- Secure disposal and data retention processes aligned to legal and business requirements.

8801 Trans-canada Hwy, Suite 500
Saint-Laurent, QC H4S 1Z6
514 331-4000
www.tfiintl.com

5.3 Secure Development & Change Management

- Secure development practices for internally developed systems.
- Change management processes to reduce operational risk.
- Controls to prevent unauthorized changes.

5.4 Awareness & Training

- Periodic training to promote cybersecurity awareness.
- Guidance on identifying and reporting potential threats.

5.5 Technology Platform Security

- Controls to protect endpoint devices, networks, and cloud platforms.
- Safeguards designed to reduce risks associated with malicious or accidental compromise.

6.0 Detect (DE)

TFI maintains capabilities to identify potential cybersecurity events and indicators of compromise.

6.1 Security Monitoring

- Centralized logging and alerting mechanisms.
- Detection of anomalous activity.
- Analysis of relevant threat intelligence.

6.2 Testing & Assessments

- Periodic assessments, including penetration testing and vulnerability scanning.
- Continuous improvement of detection capabilities based on assessment outcomes.

7.0 Respond (RS)

TFI maintains incident response processes to limit the impact of cybersecurity events and ensure appropriate coordination across the organization.

7.1 Incident Management

- Classification and escalation processes.
- Documented roles and responsibilities for incident response.
- Coordination with executive leadership and relevant stakeholders.

7.2 Communications & Reporting

- Engagement with legal and privacy resources for incidents involving regulated data.
- Notification practices consistent with legal, contractual, and regulatory requirements.

7.3 Post-Incident Review

- Analysis of incident root causes.
- Implementation of lessons learned to improve resilience and reduce future risk.

8801 Trans-canada Hwy, Suite 500
Saint-Laurent, QC H4S 1Z6
514 331-4000
www.tfiintl.com

8.0 Recover (RC)

TFI maintains recovery processes to restore operations following a cybersecurity incident.

8.1 Business Continuity & Disaster Recovery

- Resilience planning for critical systems.
- Backup and recovery practices designed to protect data availability.
- Testing of recovery capabilities to support business continuity needs.

8.2 Stakeholder Communication

- Defined channels for communication during and after recovery efforts.
- Coordination with customers, partners, and regulatory bodies when appropriate.

9.0 Continuous Improvement

TFI is committed to ongoing evaluation and improvement of its cybersecurity posture.

Continuous improvement activities include:

- Periodic evaluation of program effectiveness.
- Review of risk assessments and incident information.
- Updates to policies and standards to reflect evolving threats and technologies.
- Investment in capabilities that support risk reduction objectives.

10.0 Compliance

10.1 Regulatory and Industry Alignment

TFI's cybersecurity program is aligned to the NIST Cybersecurity Framework (NIST CSF) and supports compliance with applicable legal, regulatory, and contractual obligations in the jurisdictions where TFI International operates. These obligations may include privacy and data protection laws, financial reporting requirements, and industry-specific standards. Compliance activities are evaluated periodically to help ensure alignment with evolving requirements and expectations.

10.2 Compliance Activities

TFI evaluates compliance with applicable requirements through internal processes, including policy reviews, risk assessments, and engagement with legal and regulatory stakeholders. Affiliates support compliance by implementing controls consistent with central expectations and by addressing local regulatory obligations.

11.0 Document Maintenance

This Written Information Security Program is reviewed annually and may be updated more frequently due to significant changes in the threat landscape, business operations, or regulatory expectations.

8801 Trans-canada Hwy, Suite 500
Saint-Laurent, QC H4S 1Z6
514 331-4000
www.tfiintl.com

12.0 Approvals

Approved by the Corporate Governance & Nominating Committee and ratified by the Board of Directors

On December 11, 2025

(signed) *Josiane M Langlois*

Corporate Secretary

8801 Trans-canada Hwy, Suite 500
Saint-Laurent, QC H4S 1Z6
514 331-4000
www.tfiintl.com