1er novembre 2025

Programme écrit de sécurité de l'information

Table des matières

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

1.0 Objet

Le présent Programme écrit de sécurité de l'information (le « WISP » pour *Written Information Security Program*) décrit les principes et la structure de gouvernance par lesquels TFI International gère les risques de cybersécurité, protège les actifs d'information et soutient la résilience de l'entreprise. Le WISP s'aligne sur la version 2.0 du cadre de cybersécurité du NIST (NIST CSF) et reflète l'engagement de TFI International à sauvegarder les données qui lui sont confiées par les clients, les employés, les partenaires et les actionnaires.

Le WISP établit l'approche de gouvernance, la philosophie de gestion des risques et les capacités fondamentales de cybersécurité qui orientent les attentes en matière de contrôle à l'échelle de TFI International et de ses unités d'affaires affiliées. Le WISP soutient également la conformité aux obligations légales, réglementaires et contractuelles applicables dans les juridictions où TFI International exerce ses activités.

2.0 Portée

Ce programme s'applique à toutes les entités et sociétés affiliées de TFI International, ainsi qu'à tous les systèmes, réseaux, applications, données et services infonuagiques utilisés pour mener les opérations commerciales. Il s'applique aux employés, entrepreneurs, fournisseurs de services et partenaires qui traitent ou ont accès aux actifs d'information de TFI International.

Les actifs d'information comprennent les informations commerciales confidentielles, les données des clients, les informations financières et la propriété intellectuelle, quels que soient leur format ou leur lieu de stockage.

Le WISP est appuyé par des politiques, des normes, des procédures et des lignes directrices internes qui établissent des exigences de contrôle et des pratiques de mise en œuvre détaillées.

3.0 Gouvernance de la cybersécurité (GOVERN)

3.1 Surveillance du Conseil d'administration

La cybersécurité est régie comme un élément fondamental de la gestion des risques de l'entreprise. Le Conseil d'administration est responsable de la surveillance des risques de cybersécurité, y compris :

- L'examen annuel de la posture de cybersécurité et des risques clés.
- L'évaluation de la maturité du programme et des efforts d'amélioration.
- La surveillance des initiatives majeures de cybersécurité.
- L'examen des incidents importants et de la réponse de la direction.

Le vice-président, Sécurité des TI fournit une séance d'information annuelle au Conseil d'administration et des mises à jour plus fréquentes à la haute direction.

3.2 Responsabilisation de la direction

Le vice-président, Sécurité des TI dirige le programme de gestion des risques de cybersécurité et relève du vice-président, TI, qui relève du chef de la direction financière. La haute direction est responsable de s'assurer que les stratégies, les initiatives et les investissements en matière de cybersécurité s'alignent sur les objectifs commerciaux et la propension au risque.

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

3.3 Intégration de la gestion des risques

La gestion des risques de cybersécurité est intégrée aux pratiques plus vastes de gestion des risques de TFI, y compris :

- L'évaluation des risques pour les systèmes et les données critiques.
- La priorisation des activités d'atténuation en fonction de l'impact commercial.
- L'évaluation des risques liés à la chaîne d'approvisionnement.
- L'alignement sur les exigences réglementaires applicables.

3.4 Cadre de politiques

TFI maintient un cadre central de politiques de cybersécurité, y compris :

- Le Programme écrit de sécurité de l'information.
- Les politiques et normes de cybersécurité.
- Les procédures et lignes directrices d'accompagnement.

Les sociétés affiliées appliquent ces politiques selon une approche axée sur les risques, en tenant compte du contexte commercial et des obligations réglementaires, tout en adhérant aux attentes centrales.

4.0 Identifier (ID)

TFI identifie les risques de cybersécurité pour les systèmes, les données et les opérations grâce aux pratiques suivantes :

4.1 Gestion des actifs

- L'identification des systèmes et des types de données critiques.
- L'inventaire des actifs technologiques, y compris les services infonuagiques.
- Les pratiques de classification pour orienter les efforts de protection.

4.2 Évaluation des risques

- Des évaluations périodiques pour comprendre les menaces, les vulnérabilités et l'impact commercial potentiel.
- L'évaluation des risques émergents et des changements technologiques.
- La priorisation des activités de traitement des risques en fonction de l'impact potentiel sur les opérations et les parties prenantes.

4.3 Risque lié à la chaîne d'approvisionnement

- La vérification diligente des tiers ayant accès à des données sensibles.
- Les exigences contractuelles en matière de sécurité des données et de confidentialité.
- La surveillance des fournisseurs de services critiques.

5.0 Protéger (PR)

TFI met en œuvre des mesures de protection pour protéger les données et réduire la probabilité et l'impact des événements de cybersécurité.

5.1 Contrôle d'accès et gestion des identités

- Les contrôles d'accès basés sur les rôles.
- L'authentification multifactorielle pour les accès sensibles.
- Les principes du moindre privilège et de la séparation des tâches.

5.2 Sécurité des données

- Le chiffrement des données sensibles conformément aux exigences de la politique.
- Les pratiques de traitement des données conçues pour protéger les informations confidentielles.
- Les processus de destruction sécurisée et de conservation des données alignés sur les exigences légales et commerciales.

5.3 Développement sécurisé et gestion du changement

- Les pratiques de développement sécurisé pour les systèmes développés à l'interne.
- Les processus de gestion du changement pour réduire le risque opérationnel.
- Les contrôles pour prévenir les changements non autorisés.

5.4 Sensibilisation et formation

- Une formation périodique pour promouvoir la sensibilisation à la cybersécurité.
- Des directives sur l'identification et le signalement des menaces potentielles.

5.5 Sécurité des plateformes technologiques

- Des contrôles pour protéger les appareils terminaux, les réseaux et les plateformes infonuagiques.
- Des mesures de protection conçues pour réduire les risques associés à une compromission malveillante ou accidentelle.

6.0 Détecter (DE)

TFI maintient des capacités pour identifier les événements de cybersécurité potentiels et les indicateurs de compromission.

6.1 Surveillance de la sécurité

- Des mécanismes centralisés de journalisation et d'alerte.
- La détection des activités anormales.
- L'analyse des renseignements pertinents sur les menaces.

6.2 Tests et évaluations

- Des évaluations périodiques, y compris des tests d'intrusion et des balayages de vulnérabilités.
- L'amélioration continue des capacités de détection en fonction des résultats des évaluations.

7.0 Répondre (RS)

TFI maintient des processus de réponse aux incidents pour limiter l'impact des événements de cybersécurité et assurer une coordination appropriée à l'échelle de l'organisation.

7.1 Gestion des incidents

- Les processus de classification et d'escalade.
- Les rôles et responsabilités documentés pour la réponse aux incidents.
- La coordination avec la haute direction et les parties prenantes pertinentes.

7.2 Communications et rapports

- L'engagement avec les ressources juridiques et de protection des renseignements personnels pour les incidents impliquant des données réglementées.
- Les pratiques de notification conformes aux exigences légales, contractuelles et réglementaires.

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

7.3 Examen post-incident

- L'analyse des causes fondamentales des incidents.
- La mise en œuvre des leçons tirées pour améliorer la résilience et réduire les risques futurs.

8.0 Récupérer (RC)

TFI maintient des processus de récupération pour restaurer les opérations à la suite d'un incident de cybersécurité.

8.1 Continuité des activités et reprise après sinistre

- La planification de la résilience pour les systèmes critiques.
- Les pratiques de sauvegarde et de récupération conçues pour protéger la disponibilité des données.
- Les tests des capacités de récupération pour soutenir les besoins de continuité des activités.

8.2 Communication avec les parties prenantes

- Des canaux définis pour la communication pendant et après les efforts de récupération.
- La coordination avec les clients, les partenaires et les organismes de réglementation, s'il y a lieu.

9.0 Amélioration continue

TFI s'engage à évaluer et à améliorer continuellement sa posture de cybersécurité.

Les activités d'amélioration continue comprennent :

- L'évaluation périodique de l'efficacité du programme.
- L'examen des évaluations des risques et des informations sur les incidents.
- La mise à jour des politiques et des normes pour refléter l'évolution des menaces et des technologies.
- L'investissement dans les capacités qui soutiennent les objectifs de réduction des risques.

10.0 Conformité

10.1 Alignement réglementaire et sectoriel

Le programme de cybersécurité de TFI est aligné sur le cadre de cybersécurité du NIST (NIST CSF) et soutient la conformité aux obligations légales, réglementaires et contractuelles applicables dans les juridictions où TFI International exerce ses activités. Ces obligations peuvent inclure les lois sur la protection des renseignements personnels et des données, les exigences en matière d'information financière et les normes propres à l'industrie. Les activités de conformité sont évaluées périodiquement pour aider à assurer l'alignement sur l'évolution des exigences et des attentes.

10.2 Activités de conformité

TFI évalue la conformité aux exigences applicables par le biais de processus internes, y compris l'examen des politiques, l'évaluation des risques et l'engagement auprès des parties prenantes juridiques et réglementaires. Les sociétés affiliées soutiennent la conformité en mettant en œuvre des contrôles conformes aux attentes centrales et en répondant aux obligations réglementaires locales.

11.0 Tenue à jour du document

Le présent Programme écrit de sécurité de l'information est révisé annuellement et peut être mis à jour plus fréquemment en raison de changements importants dans le paysage des menaces, les opérations commerciales ou les attentes réglementaires.

12.0 Approbations

Approuvé par le Comité de gouvernance et des mises en candidature et ratifié par le Conseil d'administration

Le 11 décembre 2025

(signé) Josiane M. Langlois

Secrétaire de l'entreprise

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