Standard VIA Rail Canada

Tierce partie
En soutien à la Politique corporative de Sécurité de l'Information (PCSI)

Propriétaire standard:	Patrick Patenaude	Date entrée en vigueur:	Lundi 22 août 2022

1 OBJECTIF

Ce Standard articule les exigences de sécurité de l'information qu'un Tiers doit respecter pour protéger les actifs informationnels de VIA Rail. Tous les Tiers de VIA Rail doivent gérer les actifs informationnels de VIA Rail afin de préserver leur disponibilité, leur intégrité et leur sensibilité.

Certains tiers peuvent avoir accès aux actifs informationnels de VIA Rail et, ce faisant, ils doivent respecter les politiques et les normes d'entreprise de VIA Rail afin de maintenir le niveau de protection des actifs informationnels de VIA Rail et de prévenir les cyberattaques sur les actifs informationnels de VIA Rail qui pourraient causer un préjudice irréparable aux affaires, aux opérations, à la réputation et à la situation financière de VIA Rail.

2 ÉTENDUE

Ce Standard s'applique à toutes les tierces parties qui fournissent à VIA Rail des actifs informationnels ou des services par lesquels elles hébergent, stockent ou accèdent aux actifs informationnels de VIA Rail. De plus, lorsqu'ils accèdent aux actifs informationnels de VIA Rail, ils doivent se conformer à la politique de sécurité de l'information de VIA Rail, aux directives, aux normes et aux matrices de sécurité.

Les tiers sont également tenus de respecter les dispositions relatives à la sécurité de l'information énoncées dans le code de déontologie de VIA Rail afin de préserver la disponibilité, l'intégrité et la sensibilité des actifs informationnels de VIA Rail et de ses actifs de haute protection.

3 DÉFINITIONS

Haute protection (HP)

les actifs qui contiennent des informations protégées telles que des informations sur les infrastructures critiques, des informations sensibles sur la sécurité et toute information sensible de par sa nature qu'elle soit marquée VIA-Renseignements personnels ou VIA-Restreint, qui est communiquée par VIA Rail à un tiers et que VIA Rail souhaite qu'un tiers garde sensible et utilise uniquement dans le cadre de sa relation avec VIA Rail.

Exemples d'actifs HP

- Les renseignements commerciaux ou concurrentiels sensibles, exclusifs ou privés de VIA Rail, y compris les renseignements de nature commerciale, industrielle, scientifique, stratégique ou technique.
- Toutes les données classées comme VIA-Internes, VIA-Restreintes et VIA-Renseignements personnels.
- Renseignements personnels (tels que définis dans la Loi sur la protection des renseignements personnels) traités par VIA Rail
- Propriété intellectuelle de VIA Rail
- formules, procédés et mécanismes
- données, plans, dessins, plans opérationnels, techniques, commerciaux, financiers ou d'investissement
- plans d'affaires et plans stratégiques opérationnels
- stratégies, plans et prévisions en matière de nouveaux produits, de marques et de marketing, alliances stratégiques, développement de nouveaux produits et domaines d'activité
- les listes de clients et leurs coordonnées, leurs besoins, leur historique d'achat, leurs tarifs, leurs spécifications et leurs préférences
- contrats et accords
- les informations juridiques, y compris celles couvertes par le secret professionnel
- transactions d'entreprise, fusions et acquisitions
- veille concurrentielle et informations sur le marché compilées pour VIA Rail
- communications internes, mémorandums, présentations
- listes de fournisseurs
- des informations sur les systèmes, l'infrastructure et les opérations informatiques de VIA Rail

- données de l'entreprise

Actifs informationnels	Toutes les données ou banques de données, les systèmes ou supports d'information, les documents imprimés, les formulaires, les installations de technologie de l'information, ou toute combinaison de ceux-ci, et y compris les technologies opérationnelles qui sont la propriété de VIA Rail
Personnel	désigne les employés, agents, consultants, sous-traitants ou représentants de la tierce partie, le cas échéant, impliqués dans la fourniture de services
Tierce partie	désigne les fournisseurs, les gouvernements, les organisations non gouvernementales ou toute autre entité (y compris leur personnel) avec lesquels VIA Rail est en relation et peut partager ses actifs de HP.
Technologies opérationnelles	(ou "OT"), le matériel et les logiciels dédiés à la détection ou à la modification de processus physiques par la surveillance et/ou le contrôle direct de dispositifs physiques tels que des soupapes, des pompes, etc. Les systèmes SCADA font partie de ces technologies.

4 RÔLES ET RESPONSABILITÉS

Les tiers doivent connaître la classification des données de VIA. Ils doivent mettre en œuvre les contrôles nécessaires tels que définis dans les normes et les matrices de VIA.

Les actifs informationnels sont identifiés, classifiés et attribués à des propriétaires de données spécifiques. Des règles et règlements adéquats concernant leur utilisation sont établis et appliqués.

L'objectif est d'établir un cadre pour la classification et la définition des contrôles appropriés de manipulation et de sécurité à appliquer aux actifs informationnels de VIA Rail. Le niveau de classification est basé sur son degré de sensibilité, de valeur et de criticité pour VIA Rail.

Tous les actifs informationnels de VIA Rail doivent être classés dans l'un des quatre (4) niveaux suivants : lors de la création, ou après la création ou l'acceptation de la propriété par le propriétaire des données.

5 Standard

Il existe quatre classifications définies utilisées à VIA. Les quatre niveaux sont :

- **VIA-Public:** Les données qui sont généralement accessibles au public et destinées à son usage. Ces données peuvent être distribuées librement à tous les employés, consultants et tiers de VIA Rail, car il n'y a aucun risque de divulgation non autorisée. Des contrôles d'accès sont nécessaires pour protéger l'intégrité des données.

- **VIA-Interne**: Les données qui ne sont pas généralement accessibles au public ou à des parties extérieures au personnel de VIA Rail. Le risque de divulgation et de préjudice pour VIA Rail est potentiellement faible. Toutefois, l'exposition de ces données n'aura que peu ou pas d'effets négatifs sur les opérations, les actifs, la réputation, la situation financière et les obligations de confidentialité de VIA Rail.

- **VIA-Restreint**: Ces données sont considérées comme des informations destinées à un usage restreint (sur la base du besoin de savoir) au sein de VIA Rail. L'accès aux données restreintes de VIA Rail comporte un niveau de risque élevé associé à ces types de données et celles-ci doivent être protégées de manière substantielle contre toute divulgation, perte ou destruction non intentionnelle ou non autorisée, car cela pourrait avoir des effets négatifs substantiels et potentiellement coûteux pour VIA Rail. L'exposition non autorisée ou la perte de données restreintes de VIA Rail pourrait contribuer à des violations légales et à des dommages à la réputation, aux finances ou à l'exploitation.

VIA - Renseignements personnels: Parce qu'elles contiennent des informations personnelles, l'accès aux données d'informations personnelles de VIA présente un niveau de risque élevé et doit être protégé de manière substantielle contre toute divulgation, perte ou destruction non intentionnelle ou non autorisée, car cela pourrait avoir des effets négatifs substantiels et potentiellement coûteux pour VIA Rail. L'exposition non autorisée ou la perte de données personnelles de VIA Rail pourrait contribuer à des fraudes, des violations légales, des dommages à la réputation, des dommages financiers et opérationnels.

Les quatre (4) niveaux de classification des données sont couverts par deux types de protection, comme spécifiée dans la DSCI et la SCSI, et en particulier le standard de traitement des données :

- Haute protection (ou "HP" pour VIA-Restreinte et VIA-Renseignements personnels)
- Protection normale (ou "NP" pour VIA-Interne et VIA-Public)

Les tiers doivent consacrer du temps et de l'énergie à l'application de contrôles standard (sur l'ensemble des actifs informationnels) et se concentrer sur des contrôles supplémentaires sur les actifs de grande valeur (HP) pour une meilleure protection, comme définis dans les CISP, CISS et CISM.

Autres niveaux de classification

Certains des niveaux de classification définis par le gouvernement canadien peuvent être utilisés dans le contexte de VIA Rail. Les documents et les données reçus par VIA Rail et classifiés comme tels (connus sous le nom de renseignements protégés et classifiés) font l'objet d'un contrôle strict et ne sont accessibles qu'à un nombre très limité d'employés en fonction des droits d'habilitation de sécurité et du principe du besoin de savoir. Veuillez noter que ces classifications sont toujours en vigueur et que leurs valeurs peuvent remplacer les classifications définies ci-dessus. Pour toute clarification, veuillez vous adresser à l'équipe de sécurité de l'entreprise.

5.1 Certifications, cadres et normes en matière de cybersécurité (s'applique à HP)

Les tiers doivent mettre en œuvre une approche globale et structurée pour protéger les actifs informationnels de VIA Rail. Leur approche doit inclure un programme de sécurité de l'information composé de politiques, de directives et de normes. Les programmes de sécurité de l'information des tierces parties doivent être alignés sur, certifiés par ou adopter les versions actuelles d'un ou plusieurs des éléments suivants :

- Cadre de cybersécurité du NIST
  - En particulier NIST CSF V1.1
- NIST Confidentialité
- Certification CSA STAR de la Cloud Security Alliance
- AICPA SOC 2 Type 2 Certification
- ISAE 3402
- Cadre de sécurité de l'information de la série ISO/IEC 27000
  - En particulier, le Standard 27002:2013 peut être considérée comme appropriée.

5.2 Exposition aux risques de sécurité

Les Tiers doivent évaluer et surveiller leur exposition aux risques de sécurité et autres menaces et prendre les mesures appropriées pour traiter les risques associés, les actifs informationnels des Tiers et les actifs informationnels de VIA Rail.

5.3 Sensibilisation à la sécurité

Le tiers doit mettre en place un programme permanent de sensibilisation à la sécurité de l'information.

5.4 Documentation du programme de sécurité

Le Tiers doit documenter son programme de sécurité de l'information et ses contrôles de sécurité dans une politique, une directive ou une norme qui peut être mise à la disposition de VIA Rail sur demande.

5.5 Programmes et méthodologies de gestion des risques

Les Tiers doivent adopter une approche globale et structurée de la gestion des risques qui identifie et atténue les risques associés à leurs actifs informatiques et à la cybersécurité, tels que :

- 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 Contrôles de sécurité

Les tiers mettent en œuvre les contrôles de sécurité suivants :

- Planifier et gérer efficacement les versions d'entreprise, les versions de produits et les processus de déploiement ;
- Processus de gestion des vulnérabilités qui permet d'identifier, d'évaluer, de traiter et de rendre compte des vulnérabilités de sécurité des systèmes et des logiciels qui fonctionnent sur ces derniers ;
- Les correctifs de sécurité et les modifications apportées aux actifs informationnels doivent être contrôlés et suivre les procédures de gestion des modifications ;
    - les procédures de gestion des changements et les fenêtres de changement opérationnel approuvées, qui, le cas échéant, peuvent être convenues entre VIA Rail et le Tiers ;
- Des environnements de développement, de test, de production et de sauvegarde séparés physiquement et logiquement pour réduire le risque d'accès ou de modifications non autorisés aux environnements de production.
- Des contrôles pour empêcher la modification de tout code appartenant à VIA Rail sans autorisation écrite préalable ;
- Norme de sauvegarde et de conservation qui définit la fréquence des sauvegardes et les cycles de conservation de toutes les données et de tous les environnements nécessaires à l'exécution de leurs services, conformément à tout accord relatif à ces services ;
- Des contrôles de détection, de prévention et de récupération des intrusions qui protègent contre les codes malveillants et maintiennent tous les logiciels et signatures antivirus à jour et en fonctionnement actif pour détecter et supprimer les logiciels malveillants ;
- Complexité des mots de passe Normes suivant les recommandations du NIST ;
- L'authentification multifactorielle ou à deux facteurs est active pour tous les accès à distance, y compris les accès VPN ;
- L'authentification multifactorielle ou à deux facteurs est active pour tous les accès aux services en nuage, sur la base d'un accès conditionnel ;
- Établir la sécurité de l'information interne, externe et du périmètre ;

5.7 Gestion et accès aux journaux de sécurité et d'exploitation

Les actifs informationnels tiers doivent être configurés avec des capacités de gestion des journaux qui :

- Suivre les transactions de sécurité et opérationnelles ;
- Suivre les incidents, les activités, l'accès à l'information ou aux programmes, et les événements du système tels que les alertes, y compris, mais sans s'y limiter, les éléments suivants;
    - les messages de la console et les erreurs du système, ainsi que les contrôles de détection, de prévention et de récupération concernant tous les aspects de la relation avec VIA Rail et les services gérés par le Tiers
- Gérer les journaux
    - Ils doivent être conservés et disponibles pendant au moins trois mois en ligne et quinze mois hors ligne ;
    - ou à des fins relationnelles ;
    - ou plus longtemps si cela est spécifié dans l'accord pertinent et si cela est requis par les lois ou les règlements applicables aux services ou à la relation du tiers.
- sont protégés contre la falsification et l'accès non autorisé (répudiation).

5.8 Disponibilité des journaux

Le tiers doit mettre ses journaux à la disposition de VIA Rail, régulièrement ou sur demande, à des fins de vérification et d'archivage.

5.9 Droits d'audit (s'applique à HP uniquement)

Pour effectuer des évaluations de sécurité, et moyennant un préavis raisonnable, le Tiers doit permettre à VIA Rail ou à ses partenaires (y compris les organismes de réglementation gouvernementaux exigeant des inspections de VIA Rail) d'accéder aux actifs HP de VIA Rail qui sont hébergés, stockés, accédés ou autrement traités dans les actifs informationnels des Tiers.

5.10 Validation de la conformité de la sécurité

Le fournisseur tiers accepte les conditions suivantes :

- Lorsqu'un rapport SOC2 de type II peut être fourni, il doit l'être chaque année ;
- Lorsqu'un rapport SOC2 de type II ne peut être fourni ;
    - Remplir chaque année le questionnaire d'évaluation des fournisseurs fourni par VIA ;
- Coopérer avec VIA et lui fournir tous les documents ou preuves nécessaires pour remplir le questionnaire d'évaluation du fournisseur ;
- Coopérer avec toute tierce partie mandatée par VIA pour effectuer l'évaluation du fournisseur.

5.11 Déficiences de sécurité

Lorsque l'assurance ou l'audit par une tierce partie démontre un écart par rapport aux exigences du présent document, le fournisseur s'engage à :

- Fournir un plan à VIA avec des actions correctives dans un délai de 30 jours civils;
- Obtenir l'approbation de VIA sur le plan;
- Effectuer les actions correctives dans les 90 jours civils suivant l'approbation de VIA;
- Fournir à VIA la preuve de l'achèvement des actions correctives;
- La non-conformité peut entraîner l'annulation du contrat

5.12 Non-conformité

Les écarts par rapport aux contrôles énoncés dans le présent document doivent être communiqués à VIA Rail.
Veuillez transmettre les demandes à **Cybersecurity_Team@viarail.ca**

5,13 Accès physique

Le fournisseur assurera la sécurité physique. Cela comprend:

- Accès physique à tout équipement qui se trouve dans les locaux du fournisseur et qui contient des informations de VIA;
- Tout dispositif de stockage mobile ou tout autre accès sur les terminaux qui permettent aux employés d'emporter potentiellement des données hors des locaux;
- Scénarios de déplacement et de stockage de données électroniques hors site (ou site chaud).

5.14 Accès à l'information

Avant de fournir des services, le fournisseur et ses employés, agents et sous-traitants susceptibles d'accéder aux actifs et aux logiciels de VIA HP doivent avoir signé des accords concernant la protection de l'accès et la sécurité des données/logiciels qui sont conformes aux conditions du présent accord.

Le fournisseur et ses employés, agents et sous-traitants doivent se conformer à VIA Rail - à ce standard et à toutes les politiques et procédures des sociétés affiliées de VIA concernant l'accès aux données, la confidentialité et la sécurité, y compris celles interdisant ou limitant l'accès à distance aux systèmes de VIA et aux actifs d'information de VIA.

5.15 Propriété de l'information

Les actifs informationnels de VIA Rail qui sont mis à la disposition de tiers demeurent la propriété exclusive de VIA Rail.

Les tiers ne doivent pas s'attendre à ce que leur vie privée soit respectée lorsqu'ils utilisent les actifs informationnels de VIA Rail, ni à ce que tout ce qui est stocké ou reçu sur les actifs informationnels de VIA Rail ou envoyé à partir de ceux-ci soit la propriété ou l'information privée des tiers.

5.16 Conformité de la tierce partie sur place avec la Standard VIA

Lorsqu'une tierce partie accède (que ce soit sur place ou par le biais d'une session à distance) aux actifs informationnels de VIA Rail ; tenter de contourner ou de passer outre les contrôles de sécurité de VIA Rail;

- Le Standard corporative de sécurité de l'information (SCSI) et la Matrice corporative de sécurité de l'information (MCSI) de VIA Rail doivent être appliqués et respectés, y compris toute instruction spécifique fournie par VIA Rail en ce qui concerne un engagement, un mandat, un accord, un accès ou un énoncé de travail spécifique ;

Il est interdit aux tiers de :

- tenter de contourner ou d'outrepasser les contrôles de sécurité de VIA Rail, y compris mais sans s'y limiter ;
  - retirer ou altérer les mesures de sécurité, les contrôles ou les systèmes installés ou configurés par VIA Rail ;
  - détruire, altérer ou chiffrer les actifs d'information de VIA Rail, par inadvertance ou avec l'intention de les rendre inaccessibles à VIA Rail.
- intercepter, écouter ou interférer avec la voix, les données ou autres communications électroniques de VIA Rail ;diffuser volontairement ou par imprudence des virus informatiques;
- agir d'une manière qui constitue une violation du droit pénal, y compris, mais sans s'y limiter ;
  - participer à un hameçonnage ou à d'autres systèmes d'accès ou de divulgation non autorisés ;
  - chercher ou obtenir un accès non autorisé aux actifs informationnels de VIA Rail ou en attaquer l'intégrité, ou tenter de le faire ;
  - diffuser volontairement ou par imprudence des virus informatiques ;
- utiliser les actifs informationnels de VIA Rail à des fins autres que celles auxquelles ils sont destinés ou que le mandat ou les services définis du tiers ;
- Il est interdit d'exploiter une entreprise personnelle ou d'effectuer des transactions commerciales sans rapport avec l'exercice de leurs fonctions définies dans le mandat de VIA Rail.

5.17 Personnel

Le Tiers est responsable des actes et des omissions de son personnel et, à ce titre, tout le personnel qui peut avoir accès aux actifs informatiques du Tiers ou qui a accès aux actifs informatiques de VIA Rail, aux installations et aux actifs HP de VIA Rail ou qui en a la responsabilité doit:

- effectuer des vérifications des antécédents et des références;
- fournir une formation et des programmes de sensibilisation à la cybersécurité appropriés ou participer aux programmes de sensibilisation à la sécurité de VIA ;
- gérer les performances de leur personnel pour s'assurer qu'elles sont conformes aux exigences de la présente norme ;

5.18 Standard et procédures d'échange d'informations

Le tiers doit utiliser les meilleures pratiques pour l'échange d'information, par exemple, utiliser des services de transfert de fichiers gérés et sécurisés lorsqu'il partage ou échange des actifs d'information de VIA Rail avec VIA Rail ou utiliser tout outil de collaboration approuvé par VIA.

5.19 Accès non autorisé

VIA doit informer ses clients et ses employés en cas de perte ou de vol de leurs données personnelles. En outre, l'accès ou la divulgation non autorisés de données non publiques constituent une violation. Le fournisseur fournira une notification dans les 48 heures suivant l'identification d'une violation.

5.20 Notification des violations

Le fournisseur doit notifier dans les 24 heures toute suspicion de violation.

La violation sera communiquée au conseiller de VIA pour la gestion de l'information et de la vie privée (**ATIP@viaRail.ca**) avec des détails et sera disponible dans les 48 heures.

6 DOCUMENTS JUSTIFICATIFS

6.1 Annexes

Le présent standard contient les annexes suivantes :

Aucun

6.2 Standards et matrices connexes

- Standard de classification des données
- Matrice de classification des données
- Base de référence en matière de sécurité
- Matrice de sécurité

6.3 Ressources

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

7 RÉFÉRENCES

- Code d'éthique
- Politique de confidentialité
- Politique de Sécurité de l'Information Corporative
- Charte InfoSec

8 LES DEMANDES D'INFORMATION

Les questions relatives à l'interprétation de cette procédure [ou directive] doivent être adressées au poste/bureau, plus particulièrement à l'attention de :

Patrick Patenaude
Conseiller principal, Gouvernance, gestion des risques et conformité
patrick_patenaude@viaRail.ca

9 L'APPROBATION ET LA RÉVISION HISTORIQUE

Le présent standard doit être revu par le propriétaire de la norme tous les 2 ans.

9.1 Approbation

Le présent standard est approuvé et entre en vigueur à la date indiquée ci-dessous :

Patrick Patenaude sr. Advisor, governance, risk management and compliance
Title of Approving Authority

Monday, 22 août 2022
Date

9.2 Historique des révisions

Version	Description du ou des changements majeurs	Date d'entrée en vigueur
3.4	*Numéro de version aligné sur le CISP*	*2020/09/14*
3.5	*Ajusté des éléments mineurs. Remplacement de should et must par shall*	*2022/08/22*
3.5.1	*Ajusté des éléments mineurs. Mise à jour de certaines versions de frameworks à appliquer*	*2023/01/24*