Investissement Québec

Politique de sécurité de l'information et de cybersécurité

(Conseil d'administration du 7 décembre 2021)
Table des matières

1 Mise en contexte

Investissement Québec (ci-après la « Société ») recueille, génère et utilise un volume important d'information de nature confidentielle, stratégique ou sensible pour accomplir sa mission.

En vertu de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, la Société doit adopter une politique qui tient compte des principes qui y sont énoncés. La présente politique complète la Politique de gouvernance et de gestion des ressources informationnelles sous l'angle de la Sécurité de l'information.

La Société souhaite protéger l'information en sa possession ou sous sa responsabilité contre les fuites de données et les différentes cybermenaces, et répondre aux exigences législatives lui étant applicables. Pour ce faire, la Société s'engage à :

1. s'adapter à l'évolution des menaces et des risques;
2. contrer les enjeux de cybersécurité internes et externes;
3. maintenir la confiance de la clientèle;
4. agir de manière concertée;
5. responsabiliser les utilisateurs et les autres personnes visées par la présente Politique.

2 Objectifs

La Politique de sécurité de l'information et de cybersécurité (ci-après la « Politique ») établit les principes directeurs en matière de Sécurité de l'information et la désignation de rôles et de responsabilités au sein de la Société.

3 Portée

La Politique s'applique aux employés de la Société, ainsi qu'aux consultants qui travaillent dans les bureaux de la Société ou ayant accès aux systèmes d'information de la Société.

4 Définitions

Actif informationnel : Une information, quel que soit son mode de transmission ou son support (physique, vidéo ou numérique), un Système d'information, acquis ou constitué par une organisation.

Cadre de gouvernance : Ensemble des documents d'encadrement de niveau stratégique, tactique et opérationnel, ainsi que les structures, rôles et responsabilités en matière de Sécurité de l'information. Ce cadre inclut notamment le système de management en Sécurité de l'information (« SMSI »).

Cyberattaque : Ensemble coordonné d'actions malveillantes conduites par l'intermédiaire du cyberespace, qui visent à endommager, à forcer ou à détourner un réseau ou un système informatique afin de commettre un acte préjudiciable.

Détenteur de l'information : Gestionnaire responsable d'une information ou d'un ensemble d'informations liées à ses fonctions au sein de la Société.

Détenteur d'un Système d'information : Gestionnaire responsable d'un Système d'information.

Sécurité de l'information : Ensemble de mesures mises en place pour assurer la protection des ressources informationnelles en conservant leur confidentialité, leur intégrité et leur disponibilité.

Système d'information : Ensemble de ressources permettant l'utilisation, la communication et la gestion de l'information, constitué des ressources matérielles (équipements, solutions, infrastructure et technologies), des processus et des ressources humaines.

5 Principes directeurs

La Société s'inspire des meilleures pratiques en matière de Sécurité de l'information et se dote des principes directeurs suivants.

5.1 Répartir les responsabilités en sécurité de l'information

Les responsabilités relatives à la Sécurité de l'information, dont la qualification de la criticité des Actifs informationnels, l'évaluation des risques, la mise en place et le suivi de l'application des mesures de sécurité, sont réparties, entre autres, parmi les Détenteurs de l'information, les Détenteurs de système et la vice-présidence, Technologies d'affaires. Cette répartition se base sur un inventaire des Actifs informationnels qui identifie notamment les Détenteurs de l'information et les Détenteurs de système pour chaque Actif informationnel. La contribution de ces détenteurs est essentielle à une saine gestion de la Sécurité de l'information.

5.2 Protéger l'information

La Société prend des mesures de sécurité appropriées pour protéger l'information tout au long de son cycle de vie, compte tenu, notamment, de sa criticité, de son utilisation et de sa localisation.

5.3 Intégrer la sécurité dès la conception

La Sécurité de l'information est abordée dès les premières réflexions d'une nouvelle initiative, ainsi qu'à toutes les étapes du cycle d'acquisition ou de conception d'un Système d'information. Le besoin d'appliquer des mesures de sécurité est évalué pour tous les volets du Système d'information.

L'environnement technologique de production d'un Système d'information utilisé pour réaliser les opérations courantes est séparé des environnements utilisés pour la conception et les essais. De plus, de l'information fictive ou anonymisée est utilisée pour concevoir, modifier ou tester un Système d'information.

5.4 Limiter l'accès aux Actifs informationnels

L'accès à un Actif informationnel doit être autorisé sur la base du besoin d'une personne d'y avoir accès afin d'assumer les responsabilités propres à ses fonctions.

5.5 Prévenir toute irrégularité

La Société met en place des mécanismes de veille et de vérification pour observer et identifier de façon proactive toute vulnérabilité ou évènement préjudiciable aux Actifs informationnels.

5.6 Répondre à un incident de Sécurité de l'information

La Société se dote d'un processus permettant de répondre sans délai aux actes préjudiciables, incidents et sinistres en Sécurité de l'information. Ce processus vise notamment à minimiser les impacts, rétablir les services et rendre à nouveau disponible l'information dans un format intègre, le cas échéant.

La Société met à jour, communique et teste périodiquement ce processus en fonction de la criticité des Actifs informationnels.

5.7 Vérifier la conformité

La Société se dote d'indicateurs de gestion et de performance permettant de mesurer la conformité du Cadre de gouvernance en regard du niveau de maturité visé en Sécurité de l'information. Des actions sont prises afin de remédier à toute non-conformité dans les plus brefs délais.

6 Activités

L'application des principes directeurs est soutenue par la mise en œuvre d'un Cadre de gouvernance et d'un programme de formation et de sensibilisation.

6.1 Cadre de gouvernance de la sécurité de l'information

Le Cadre de gouvernance de la Sécurité de l'information définit une structure de coordination et détermine l'encadrement de niveau stratégique, tactique et opérationnel. La structure de coordination repose sur l'interaction entre la direction, les comités et les rôles de niveau tactique.

Il s'appuie sur les meilleures pratiques, les normes internationales, ainsi que sur les référentiels de contrôles de sécurité reconnus, ceux-ci devant être identifiés dans les directives en appui à la présente Politique.

6.2 Système de management de la Sécurité de l'information (SMSI) :

Le SMSI est constitué des mesures et des processus en matière de Sécurité de l'information visant à préserver la confidentialité, l'intégrité et la disponibilité de l'information. Il définit notamment les activités de coordination, de contrôle et d'amélioration continue dans le but de protéger les Actifs informationnels.

Un plan d'action triennal en Sécurité de l'information est ajusté annuellement et permet de planifier et suivre les activités de mise en œuvre graduelle du SMSI.

6.3 Formation et sensibilisation

Des activités de formation et de sensibilisation responsabilisent le personnel au respect des obligations de Sécurité de l'information et à l'adoption d'un comportement exemplaire en matière de Sécurité de l'information. La formation et la sensibilisation visent à augmenter la vigilance des employés et ainsi réduire le risque lié au comportement de ceux-ci (ex. : hameçonnage).

Une violation réelle ou présumée des obligations de Sécurité de l'information contrevient aux dispositions du Code d'éthique et l'auteur s'expose, selon la nature et la gravité de la faute, à des mesures disciplinaires ou des sanctions.

7 Rôles et responsabilités

7.1 Conseil d'administration :

- approuve la présente Politique et toute modification à celle-ci;
- évalue l'efficacité de la Politique, du Cadre de gouvernance de la Sécurité de l'information et de ses composantes.

7.2 Comité de direction (CODIR) :

- adopte le Cadre de gouvernance et le plan d'action triennal, qui inclut notamment les priorités en Sécurité de l'information, et approuve toute directive reliée à la présente Politique;
- veille à l'adéquation des mesures de sécurité de l'information déployées par rapport aux risques encourus;
- approuve la Charte du Comité de sécurité et toute modification à celle-ci;
- recommande l'adoption de la présente Politique au Conseil d'administration.

7.3 Comité de sécurité :

- soutient le Comité de direction dans ses responsabilités à l'égard de la Sécurité de l'information;
- examine le Cadre de gouvernance, les modifications à la présente Politique et les directives de sécurité et soumet ses recommandations au CODIR;
- approuve le programme de formation et de sensibilisation en matière de Sécurité de l'information;
- examine les suivis concernant le plan d'action triennal, la surveillance, les dérogations, les incidents, les risques et la conformité.

7.4 Vice-président, Technologies d'affaires (« VPTA »):

- agit à titre de Chef délégué de la sécurité de l'information (CDSI);
- veille à la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable pour la Société;
- assure la mise en œuvre du Cadre de gouvernance;
- désigne, parmi les membres de son personnel, des responsables pour des domaines spécifiques en matière de Sécurité de l'information et s'assure, selon le contexte et avec les adaptations nécessaires, du maintien d'un lien fonctionnel entre ceux-ci et le CSIO.

7.5 Directeur principal, Sécurité de l'information :

- assume le rôle de Chef de la sécurité de l'information organisationnelle (CSIO);

- agit à titre de responsable tactique et opérationnel de la Sécurité de l'information et de coordonnateur de la mise en œuvre des actions en Sécurité de l'information;
- préside le Comité de sécurité;
- est responsable de l'implantation du Cadre de gouvernance de sécurité;
- propose au VPTA ou au Comité de sécurité le Cadre de gouvernance, le plan d'action triennal, les directives et les modifications appropriées;
- assiste les Détenteurs de l'information dans la catégorisation de l'information sous leur responsabilité et tient à jour un registre d'autorité (registre d'entreprise de catégorisation de l'information);
- assiste les Détenteurs de l'information et les Détenteurs de système dans la réalisation d'exercices de gestion de risques de Sécurité de l'information, recommande l'application des mesures d'atténuation conséquentes et en assure le suivi;
- met en place, dirige, opérationnalise et contribue à l'évolution de l'offre de services d'un Centre opérationnel de cyberdéfense (COC);
- met en place les outils et mesures de Sécurité de l'information requis pour l'accomplissement des activités opérationnelles en Sécurité de l'information, notamment la gestion des accès et la surveillance, selon les besoins des Détenteurs de l'information;
- s'assure que la Sécurité de l'information est considérée dès le début de la conception d'un Système d'information et recommande les mesures appropriées à prendre en compte en matière de Sécurité de l'information lors de toute vérification préalable à l'intégration d'un Système d'information;
- élabore un programme de formation et de sensibilisation et coordonne son application;
- coordonne la réalisation périodique de tests d'intrusion et de vulnérabilités;
- coordonne la réalisation périodique de vérifications de conformité à la Sécurité de l'information et s'assure que des actions sont prises pour remédier aux non-conformités;
- s'assure de la prise en charge de tout incident de Sécurité de l'information et avise, sans délai, le CDSI lorsqu'un incident de sécurité cause ou peut causer un préjudice important à la Sécurité de l'information, ainsi qu'à tout autre équipe selon la nature de l'incident (Communications, Gestion des risques, Affaires juridiques, etc.);
- coordonne l'élaboration du plan permettant de rendre à nouveau disponible l'information intègre et de qualité requise par un service jugé critique, à la suite d'un incident, et ce, dans le délai de résilience préalablement convenu.

7.6 Détenteur de l'information :

- catégorise l'information, ce qui consiste à évaluer sa valeur, en termes de confidentialité, d'intégrité et de disponibilité dans le but de déterminer le niveau de protection requis;
- s'assure que l'information, sous sa responsabilité, bénéficie d'un niveau de protection proportionnel à sa valeur tout au long de son cycle de vie;
- autorise les accès à une information sous sa responsabilité et indique si des mesures de contrôle préventives doivent être appliquées;
- en collaboration avec la vice-présidence, Gestion des risques et la Sécurité de l'information, participe activement au processus de mitigation des risques;
- au besoin, transmet une demande d'avis de Sécurité de l'information concernant l'utilisation de l'information dans un contexte particulier;
- est informé d'un incident qui concerne la Sécurité de l'information sous sa responsabilité;
- s'assure du suivi et de l'application des mesures de sécurité recommandées par la Sécurité de l'information;
- s'assure que l'information sous sa responsabilité fait partie du registre d'autorité.

7.7 Détenteur d'un Système d'information :

- autorise les accès associés à un Système d'information en respect de la séparation des tâches incompatibles;
- autorise les mesures de sécurité recommandées dans le dossier de sécurité d'un Système d'information;
- autorise explicitement la mise en service (en opération) d'une nouveauté, d'un changement ou d'une amélioration qui respecte les exigences de Sécurité de l'information convenues;
- contribue à identifier des stratagèmes de comportement irréguliers devant faire objet de surveillance;
- s'assure d'une révision périodique des habilitations de rôles ou d'accès à l'information sous sa responsabilité;

- s’assure que le Système d’information et les actifs informationnels sous sa responsabilité font partie du registre d’autorité;
- en collaboration avec le Détenteur de l’information, vérifie périodiquement si l’utilisation de l’information soulève un risque d’incidence sur la Sécurité de l’information, auquel cas, il autorise des mesures de sécurité permettant d’atténuer ce risque et effectue un suivi de leur application sur les actifs informationnels au moment requis;
- s’assure que la Sécurité de l’information est abordée dès les premières réflexions d’une nouvelle initiative ou innovation ainsi qu’à toutes les étapes du cycle de conception d’un Système d’information;
- applique toute mesure de sécurité autorisée par un Détenteur de l’information;
- autorise la mise en opération d’un Système d’information sous sa responsabilité, et ce, après avoir pris connaissance du résultat des vérifications de la Sécurité de l’information.

7.8 Pilote de Système d’information

a) Assiste le Détenteur d’un Système d’information dans l’exercice de ses responsabilités en SI. À ce titre, il :

- participe à toutes les étapes menant à la mise en place d’un nouveau Système d’information ou tout changement ou évolution;
- contribue à chaque activité associée aux responsabilités du Détenteur de processus d’affaires, sans participer aux processus décisionnels.

7.9 Gestionnaire

- s’assure du respect des mesures de sécurité applicables aux Actifs informationnels sous sa responsabilité;
- autorise des privilèges d’accès logiques et physiques détenus par les employés et consultants sous sa supervision.

7.10 Utilisateur

- protège l’information mise à sa disposition lorsqu’il l’utilise, avec discernement et aux seules fins permises, et ce, conformément à la présente Politique et tout document qui en découle et au Code d’éthique des employés et dirigeants et de ses filiales en propriété exclusive;
- signale au Centre des services des utilisateurs (CSU) tout acte ou comportement qui compromet ou peut compromettre la sécurité des Actifs informationnels;
- effectue les formations prescrites, se responsabilise en Sécurité de l’information et adopte un comportement exemplaire en matière de cybersécurité.

8 Révision

La présente Politique est sous la responsabilité du vice-président, Technologies d’affaires. Il veille à ce que la Politique soit révisée en temps opportun, mais au plus tard à tous les trois ans.

9 Approbation

Le conseil d’administration approuve la présente Politique sur recommandation du Comité de direction.