Investissement Québec

P1503

ManuelGestion

Imprimez noir et blanc

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Table des matières

1. Mise en contexte et objectif

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.

L'évolution rapide des technologies numériques, notamment l'intelligence artificielle, l'infonuagique, l'automatisation avancée et l'intégration accrue de services technologiques tiers, transforme le paysage des risques informationnels. La Société reconnaît que ces innovations requièrent un encadrement spécifique afin d'assurer une utilisation sécuritaire, responsable et conforme aux obligations légales et éthiques.

De plus, 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 transformation numérique de la Société s'appuie notamment sur des services infonuagiques, des plateformes technologiques externes et des environnements hybrides. Cette réalité exige une gestion rigoureuse des risques liés à la dépendance aux fournisseurs, à la localisation des données, à la résilience opérationnelle et à la sécurité des configurations.

La Politique de sécurité de l'information (ci-après la « Politique ») vise, par conséquent, à assurer la protection des actifs informationnels de l'organisation en garantissant la confidentialité, l'intégrité et leur disponibilité. Elle a pour objectif de prévenir, détecter et gérer les incidents de sécurité, tout en encadrant l'accès et l'utilisation des systèmes et des informations selon les rôles et responsabilités. Elle contribue également à assurer la conformité aux exigences légales, réglementaires et normatives applicables, tout en sensibilisant les utilisateurs aux bonnes pratiques en matière de sécurité. Enfin, cette politique s'inscrit dans une démarche d'amélioration continue afin d'adapter les mesures de protection aux risques et aux menaces en constante évolution.

Elle s'appuie sur une approche structurée de gestion des risques afin d'assurer une protection proportionnée aux enjeux de l'organisation et s'inspire notamment des référentiels reconnus en matière de sécurité de l'information et de cybersécurité, incluant les cadres publiés par le National Institute of Standards and Technology (NIST) et le Centre canadien pour la cybersécurité, et tient compte des exigences propres aux environnements infonuagiques et hybrides.

2. Portée

La présente Politique s'applique à tous les employés de la Société, partenaires et fournisseurs ayant accès aux actifs informationnels de l'organisation, incluant les données, systèmes et équipements, peu importe le lieu ou le mode d'accès.

3. 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 »).

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.

Intelligence artificielle (IA) : Système technologique qui, de manière autonome ou partiellement autonome, traite des données liées à l'activité humaine par l'utilisation d'algorithmes génétiques, de réseaux neuronaux, d'apprentissage automatique ou d'autres techniques pour générer du contenu, faire des prédictions ou des recommandations ou prendre des décisions.

IA générative : Fait référence aux systèmes d'IA dont l'objectif principal est de créer de nouveaux contenus comme du texte, des images, des audios et des vidéos.

Infonuagique : Modèle de prestation de services technologiques permettant l'accès à des ressources informatiques mutualisées (infrastructure, plateforme, logiciel) via un réseau.

Responsabilité partagée : Principe selon lequel la sécurité d'un service infonuagique est répartie entre le fournisseur et l'organisation cliente.

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.

SMSI : Le système de management de la sécurité de l'information 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.

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.

4. Principes

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

Adopter une approche basée sur les risques

La Société adapte ses mesures de sécurité en fonction de la criticité des actifs informationnels ainsi que de l'évolution des menaces et des vulnérabilités.

Assurer la protection des actifs informationnels

La Société met en œuvre des mesures visant à préserver la confidentialité, l'intégrité et la disponibilité de l'information, quels que soient les environnements dans lesquels elle est traitée.

Favoriser une gouvernance intégrée et concertée

La sécurité de l'information repose sur une collaboration entre les différentes fonctions de l'organisation, soutenue par des rôles et responsabilités clairement définis.

Responsabiliser les utilisateurs et les parties prenantes

Toute personne ayant accès aux actifs informationnels doit adopter des comportements conformes aux exigences de sécurité et contribuer à leur protection, en étant responsable de ses actions à cet égard.

S'améliorer en continu

La Société révise et améliore ses pratiques de sécurité de l'information afin de s'adapter à l'évolution des menaces, des risques, des technologies et des exigences réglementaires.

5. Activités

L'application des principes directeurs est soutenue par un ensemble structuré d'activités visant à assurer la protection des actifs informationnels. Ces activités couvrent la gouvernance, l'identification, la protection, la détection, la réponse et le rétablissement, dans une perspective d'amélioration continue.

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.

Les politiques, directives et autres documents d'encadrement en appui à la présente Politique sont présentés au Manuel de gestion.

5.1 Gouvernance de la sécurité de l'information

5.1.1 Cadre de gouvernance

La Société met en place un cadre de gouvernance de la sécurité de l'information définissant les structures, les rôles, les responsabilités et les mécanismes de coordination nécessaires à une gestion efficace, couvrant les niveaux stratégiques, tactiques et opérationnels, et alignés sur ses objectifs organisationnels et son appétit pour le risque. Ce cadre s'appuie sur des normes, des référentiels, dont la NIST 800-53 r5, et des meilleures pratiques reconnus en matière de sécurité de l'information. En ce sens, la Société réalise périodiquement une évaluation de maturité de la sécurité de l'information, notamment selon une approche de type CMMI, alignée sur ce cadre NIST (incluant le NIST CSF), afin d'évaluer l'efficacité de ses contrôles et d'orienter ses plans d'amélioration continue.

Il inclut le système de management de la sécurité de l'information (SMSI) visant à assurer la planification, la mise en œuvre, le suivi et l'amélioration continue des mesures de sécurité. Le SMSI permet notamment de coordonner les activités, de suivre la performance et d'assurer une gestion cohérente des risques liés à la sécurité de l'information.

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.

La Société se dote d'indicateurs permettant d'évaluer l'efficacité de son cadre de gouvernance, son niveau de maturité et sa posture de sécurité, et d'orienter ses actions. Des actions sont prises afin de remédier à toute situation de non-conformité dans les plus brefs délais.

Les responsabilités relatives à la sécurité de l'information, incluant notamment la catégorisation des actifs informationnels, l'évaluation des risques ainsi que la mise en place et le suivi des mesures de sécurité, sont réparties entre les différentes fonctions de l'organisation, incluant les détenteurs de l'information, les détenteurs de systèmes d'information et la PVP Technologies d'information. Cette répartition s'appuie sur un inventaire des actifs informationnels permettant d'identifier, pour chacun d'eux, les responsables désignés.

5.1.2 Gestion des risques

La Société applique une approche structurée de gestion des risques en sécurité de l'information, permettant d'identifier, d'analyser, d'évaluer et de traiter les risques susceptibles de compromettre les actifs informationnels. Les risques significatifs font l'objet d'un suivi tel que décrit dans la section reddition de comptes.

Elle s'assure que les risques cybernétiques significatifs sont intégrés à son registre opérationnel des risques et font l'objet d'un suivi au niveau de la haute direction.

Elle encadre les risques liés aux tiers, aux services infonuagiques et aux technologies émergentes, en s'assurant qu'ils font l'objet d'une gouvernance appropriée, de mécanismes de suivi et d'exigences de sécurité adaptées. Le développement, l'intégration et l'utilisation des systèmes d'intelligence artificielle sont encadrés conformément aux cadres organisationnels applicables. Quant aux environnements infonuagiques, ils font l'objet d'une gestion des risques adaptée et proportionnée, notamment en ce qui concerne le modèle de responsabilité partagée.

5.2 Identification des actifs informationnels et des risques liés aux actifs

La Société identifie et maintient un inventaire et un registre d'autorité associé aux actifs informationnels, incluant les systèmes d'information, les données et les ressources technologiques qui les soutiennent. Cet inventaire permet de soutenir la prise de décision et l'application de mesures de sécurité appropriées.

La Société procède à la catégorisation des actifs informationnels en fonction de leur valeur, de leur sensibilité et de leur criticité, afin de déterminer les exigences de protection applicables et de prioriser les actions en matière de sécurité de l'information.

Elle maintient une connaissance adéquate de ses environnements technologiques et des facteurs susceptibles d'affecter ses actifs informationnels, incluant les menaces, les vulnérabilités, les dépendances technologiques et les composantes tierces.

Cette connaissance est soutenue notamment par la mise à jour des informations relatives aux actifs, aux services infonuagiques et aux fournisseurs, ainsi que par la réalisation périodique d'évaluations de risques, afin de soutenir l'identification proactive des risques et des faiblesses de sécurité.

Afin d'assurer une saine gouvernance de ses actifs, la Société maintient à jour:

- un inventaire des services infonuagiques utilisés ;
- une classification des environnements selon leur degré de criticité ;
- un registre des fournisseurs technologiques ;
- un processus d'évaluation périodique des risques liés aux actifs et services associés
- l'évaluation des certifications et attestations des fournisseurs ;
- le processus de validation des clauses contractuelles de sécurité ;
- l'exigence de notification d'incident pour nos actifs et chez les partenaires.

La Société peut mandater périodiquement une évaluation indépendante de sa posture de sécurité afin de valider son niveau de maturité et identifier des pistes d'amélioration.

5.3 Protection des actifs informationnels

La Société met en place des mesures de sécurité appropriées afin d'assurer la protection des actifs informationnels tout au long de leur cycle de vie, en fonction de leur criticité, de leur localisation, de leur utilisation et des risques auxquels ils sont exposés. Ces mesures visent à préserver la confidentialité, l'intégrité et la disponibilité de l'information.

Ces mesures visent entre autres à:

- prévenir le transfert non autorisé d'information sensible ;
- détecter les comportements anormaux de transmission ;
- encadrer le partage externe via courriel, plateformes collaboratives ou services infonuagiques ;
- surveiller l'utilisation d'outils d'intelligence artificielle pouvant entraîner une divulgation involontaire d'information;
- assurer la capacité de réversibilité et de récupération des données chez les fournisseurs qui les hébergent.

La Société s'assure que les exigences de sécurité et de conformité sont prises en compte dès la phase de planification des projets et lors de toute évolution des systèmes. Des mesures appropriées sont mises en place afin d'assurer une séparation adéquate des environnements, ainsi que l'utilisation de données fictives ou anonymisées dans les contextes de développement et d'essai.

Elle applique ainsi des principes reconnus, tels que la protection des renseignements personnels dès la conception, la sécurité par défaut et des approches d'architecture sécuritaire adaptées aux risques.

Toute initiative impliquant des services infonuagiques ou des technologies émergentes fait l'objet d'une analyse de sécurité appropriée, incluant l'évaluation des risques, des dépendances technologiques et des enjeux de réversibilité.

Les architectures technologiques doivent utiliser un modèle de sécurité de type « Zero Trust », où aucun utilisateur, appareil ou service n'est implicitement considéré comme fiable, indépendamment de son emplacement réseau.

5.3.1 Gestion des accès logiques

L'accès aux actifs informationnels est accordé sur la base du besoin d'en connaître et du principe du moindre privilège. La Société encadre la gestion du cycle de vie des identités numériques et met en place des mécanismes d'authentification et de contrôle d'accès adaptés aux risques, incluant, lorsque requis, des mécanismes d'authentification renforcée en fonction de la sensibilité des actifs informationnels et des privilèges accordés. Les accès administratifs aux différents systèmes doivent faire l'objet d'une gestion distincte des privilèges associés.

5.3.2 Sécurisation des environnements physiques

La Société met en place des mesures de sécurité physique appropriées afin de protéger les actifs informationnels contre tout accès, utilisation, divulgation, altération ou destruction non autorisés. Ces mesures incluent notamment :

- le contrôle des accès aux installations;
- la protection des équipements et des supports d'information;
- la protection des environnements physiques où sont traitées ou entreposées des informations.

La direction de la gestion immobilière (DGI) est responsable, par l'entremise de sa Directive sur la sécurité physique, de la mise en place, de l'exploitation et du maintien des contrôles d'accès

physiques aux bureaux et aux installations de la Société, en coordination avec les équipes de sécurité de l'information.

5.3.3 Sécurisation des environnements infonuagiques

Lorsqu'un actif informationnel est hébergé dans un environnement infonuagique, la Société s'assure que :

- les données doivent être chiffrées en transit et au repos selon des standards reconnus;
- la gestion des clés cryptographiques soit encadrée ;
- la localisation des données soit connue et documentée ;
- l'accès privilégié soit limité, surveillé et périodiquement revu.

5.3.4 Prévention des fuites de données

La Société met en place des mesures visant à prévenir la perte, l'exfiltration, la divulgation non autorisée, la modification ou l'utilisation abusive de l'information, notamment par l'encadrement des flux de données, des mécanismes de partage et des usages technologiques. Elle encadre également l'utilisation des technologies, incluant les services infonuagiques et les solutions d'intelligence artificielle, afin de prévenir l'utilisation non autorisée de tels outils et toute divulgation involontaire d'information.

5.3.5 Formation et responsabilisation

La Société met en œuvre des activités de formation et de responsabilisation obligatoires pour l'ensemble des employés et des consultants, selon les rôles et responsabilités qui leur sont attribués et l'évolution des risques visant à assurer que les membres du personnel comprennent leurs responsabilités en matière de sécurité de l'information et adoptent des comportements sécuritaires dans l'exercice de leurs fonctions. Ces activités visent notamment à :

- renforcer la vigilance face aux menaces;
- assurer les bonnes pratiques en matière de sécurité de l'information;
- réduire les risques liés au facteur humain;
- promouvoir le respect des obligations organisationnelles en matière de sécurité de l'information.

Les exigences de formation et de responsabilisation sont définies et adaptées en fonction des rôles, des responsabilités et de l'évolution des risques. Toute violation des obligations en matière de sécurité de l'information peut, selon la nature et la gravité du cas, entraîner une sanction disciplinaire ou une mesure administrative qui peut inclure une réprimande, une suspension ou un congédiement, et ce, conformément aux dispositions des encadrements internes de la Société et des conventions collectives ou autres ententes applicables, le cas échéant.

5.4 Détection des événements de sécurité

La Société met en place des mécanismes de surveillance et de détection visant à identifier de manière proactive les événements de sécurité, les vulnérabilités et les activités ou comportements anormaux susceptibles de compromettre la sécurité de l'information.

Ces mécanismes permettent de détecter une compromission, une utilisation abusive des actifs informationnels ou des tentatives d'usurpation ou de fraude numérique.

Ces derniers incluent, sans s'y restreindre :

- la surveillance des systèmes d'information, des accès et des flux de données;
- la détection d'anomalies;
- la collecte, la centralisation et l'analyse des journaux d'événements ainsi que l'analyse des comportements;
- l'évaluation périodique de la posture de sécurité;
- l'utilisation d'outils d'intelligence artificielle non autorisés;
- les risques de fraude par usurpation numérique (ex. : hypertrucage, voix synthétique);
- les comportements anormaux liés à l'automatisation, une tentative d'exfiltration ou d'utilisation abusive d'information;
- la surveillance des vulnérabilités logicielles, des dépendances applicatives et des composantes tierces intégrées aux systèmes d'information.

Les mécanismes de surveillance et de détection s'appliquent à l'ensemble des environnements technologiques de la Société, incluant les environnements infonuagiques et les composantes tierces. Ils permettent notamment d'identifier les faiblesses de configuration, les vulnérabilités, les comportements inhabituels et d'évaluer la posture de sécurité.

Ces activités sont réalisées dans le respect des lois et règlements applicables, notamment celles relatives à la protection des renseignements personnels et au droit à la vie privée.

5.5 Réponse aux incidents de sécurité

La Société applique un processus structuré de gestion des incidents et de crise, incluant ceux de sécurité de l'information, permettant d'intervenir de manière diligente lors de la survenance d'un événement de sécurité. Ce processus vise à détecter, signaler, analyser, contenir et traiter les incidents, à en limiter les impacts et à assurer la coordination des interventions.

Le processus de gestion d'incident et de crise est communiqué aux parties prenantes concernées, mis à jour de façon périodique et fait l'objet d'exercices de validation en fonction de la criticité des actifs informationnels.

La Société s'assure que les incidents impliquant des technologies émergentes, incluant les systèmes d'intelligence artificielle, font l'objet d'une analyse appropriée tenant compte de leurs spécificités, notamment en matière de qualité des résultats, de protection des données et d'intégrité des systèmes.

5.6 Continuité des activités et rétablissement

La Société met en place un programme de continuité de ses activités et la reprise de ses services à la suite d'un incident de sécurité ou d'un sinistre affectant ses actifs informationnels. Ce programme est mis à jour, communiqué et testé périodiquement en fonction de la criticité des actifs informationnels.

Pour y parvenir, la Société tient compte des dépendances organisationnelles et technologiques, incluant les services infonuagiques et les fournisseurs externes, et visent à assurer la disponibilité, l'intégrité et la récupération de l'information dans des délais compatibles avec les exigences opérationnelles.

De plus, la Société met en place des mesures de résilience technologique appropriées, incluant des mécanismes de sauvegarde des données critiques, des capacités de reprise indépendantes et des

stratégies permettant de réduire les impacts liés à la dépendance envers des fournisseurs ou des environnements technologiques spécifiques.

6. Rôles et responsabilités

Le Conseil d'administration :

- approuve la Politique, sur recommandation du comité de gestion des risques.

Le Comité de gestion des risques du CA (CGR-CA) :

- recommande au conseil d'administration l'approbation de la Politique;
- reçoit la reddition de comptes prévue dans la Politique.

Le Comité de direction (CODIR) :

- approuve le SMSI et le plan triennal;
- approuve les directives découlant de la présente Politique;
- veille à l'adéquation des mesures de sécurité de l'information déployées par rapport aux risques encourus;
- recommande au CGR-CA l'adoption de la présente politique subséquente au CA.

La Première vice-présidence, Technologies de l'information :

- assure la mise en application, la mise à jour et le suivi des encadrements sous sa responsabilité et du Cadre de gouvernance de sécurité;
- dépose et recommande au CODIR l'approbation du SMSI et le plan triennal;
- examine les suivis concernant le plan d'action triennal, la surveillance, les dérogations, les incidents, les risques et la conformité;
- agit à titre de Chef délégué de la sécurité de l'information (CDSI);
- veille à la mise en place et l'efficacité des mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable et déterminé pour et par la Société;
- nomme le Responsable de la sécurité de l'information (RSI) aussi connu sous l'acronyme CISO.

La Direction principale, Sécurité de l'information :

- assume le rôle de Responsable de la sécurité de l'information (RSI/CISO);
- agit à titre de responsable tactique et opérationnel de la sécurité de l'information et la mise en œuvre des actions en sécurité de l'information;
- est responsable de l'implantation du Cadre de gouvernance de sécurité;
- propose au PVPTI le Cadre de gouvernance, le plan d'action triennal, les directives et les modifications appropriées;
- élabore et coordonne la diffusion et l'application d'un programme de formation et de responsabilisation et coordonne son application;
- 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 (SOC);

- 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;
- coordonne la réalisation périodique de tests d'intrusion et de vulnérabilités;
- coordonne la réalisation périodique de vérification 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, dès que possible, le CDSI lorsqu'un incident de sécurité cause ou peut causer un préjudice important à la Sécurité de l'information, ainsi qu'à toute autre équipe selon la nature de l'incident (Communications, Gestion des risques, Affaires juridiques, etc.);
- s'assure de la mise en œuvre d'un programme de surveillance continue des systèmes ;
- valide les exigences de sécurité applicables aux contrats ;
- coordonne les évaluations de posture de sécurité;
- coordonne les exercices de simulation d'incidents;
- coordonne la mise à jour en continu du registre d'autorité
- met en place un processus d'évaluation des risques applicatifs;
- veille à la surveillance des usages technologiques émergents;
- met en place un programme organisationnel de prévention des pertes de données.

La Vice-présidence, Talent et relation employé

- effectue les vérifications de pré-emploi requises incluant la vérification des antécédents lorsque applicable, dans le cadre du processus d'embauche des employés et des consultants externes. À l'issue de ces vérifications, elle confirme l'autorisation et l'admissibilité des personnes à travailler pour la Société, conformément aux exigences en vigueur.

Le 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 contrôles préventives doivent être appliquées;
- en collaboration avec la vice-présidence, gestion intégrée des risques d'entreprise et la Direction principale, 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;
- lorsqu'il est informé d'un incident concernant la sécurité de l'information sous sa responsabilité, il doit déclarer l'incident au CSU et collaborer à sa résolution;
- 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.

Le 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.

Le pilote de système d'information:

- assiste le détenteur d'un système d'information dans l'exercice de ses responsabilités en SI;
- 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.

Le 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.

L'utilisateur:

- protège l'information mise à sa disposition en l'utilisant, avec discernement et aux seules fins permises, et ce, conformément à la présente Politique et tout encadrement qui en découle, ainsi qu'au Code d'éthique des employés et dirigeants d'Investissement Québec et de ses filiales;
- 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.

7. Reddition de comptes

Une reddition de compte est produite par le CISO, annuellement ou au besoin, au CGR-CA sur le niveau de maturité de la sécurité incluant :

- les risques résiduels spécifiques à celui-ci;
- les priorités d'affaires qui y sont associées;
- les actions entreprises en matière de sécurité afin de mitiger le risque et le rendre acceptable au niveau de l'organisation.

8. Révision, approbation

La Politique entre en vigueur au moment de son approbation par le C. A. et doit être révisée tous les trois (3) ans ou plus fréquemment si d'autres considérations le justifient.

Titre : Politique de sécurité de l'information [Référence : P1503.pdf]
PVP Responsable : PVPTI

Date de création :
2021-11-01
Première entrée en vigueur :
2021-12-07
Date de dernière révision :
2026-05-21
Adoptée par : Conseil d'administration
Date d'approbation : 2021-12-07; 2026-05-21