Sujet :	Politique générale de la sécurité de l'information
Responsable :	Division des Technologies de l'information Gestion des risques et sécurité des technologies de l'information
Adoptée par le CA :	6 septembre 2023
En vigueur :	6 septembre 2023

1.CONTEXTE

La SAQ traite de l'information qui peut être de nature confidentielle, stratégique et sensible et qui implique plusieurs parties prenantes, telles que les employés, les clients et les fournisseurs. Le succès de la SAQ repose sur une exploitation adéquate de ces informations. Elle reconnaît donc l'importance de les protéger et met en œuvre un cadre de gestion de la sécurité de l'information.

La Politique générale de sécurité de l'information (« la Politique ») vise à assurer la confidentialité, l'intégrité et la disponibilité des informations de la SAQ. Les mesures de sécurité qu'elle établit tiennent compte de la nature, de l'importance et de l'utilisation de l'information, des priorités d'affaires de la SAQ, ainsi que des risques liés à ses activités.

La Politique s'applique dans le respect des lois et des obligations auxquelles la SAQ est assujettie, notamment :

- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
- La norme de sécurité de l'industrie des cartes de paiement (PCI-DSS);
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03).

2. DÉFINITIONS

Dans la présente Politique, on entend par :

« Information » : Ensemble de données ou informations appartenant à la SAQ qui doivent être protégées, et ce, quel que soit la forme, le support, le dispositif ou l'emplacement. Certaines politiques gouvernementales y font référence sous le terme d'actif informationnel.

« Information critique »: Ensemble des informations confidentielles ainsi que les systèmes critiques dont la divulgation, l'altération, la perte ou la destruction sont susceptibles de porter préjudice et d'entraîner des conséquences néfastes sur les opérations de la SAQ. Ces informations nécessitent une disponibilité contrôlée, une grande intégrité et un niveau de confidentialité élevé, soit un accès exclusif aux personnes autorisées.

« Cycle de vie » : Ensemble des étapes constituant la vie d'une information. Cela comprend la création, la collecte, la consultation, l'utilisation, la sauvegarde, la conservation, la communication, le transfert et la destruction.

« Propriétaire d'information » : Toute personne désignée responsable d'une information appartenant à la SAQ ou qui lui a été confiée.

« Intégrité » : Propriété d'une donnée ou information qui n'a subi aucune altération non autorisée durant son cycle de vie.

« Renseignements personnels » : Toute information qui concerne une personne physique et qui permet de l'identifier directement ou indirectement.

« Risque de sécurité de l'information » : Ensemble des situations susceptibles de mettre à risque la confidentialité, la disponibilité et l'intégrité des informations de la SAQ, et par conséquent, d'entraîner des conséquences néfastes sur ses opérations.

« Sécurité de l'information » : Ensemble des mesures permettant d'assurer la confidentialité, la disponibilité et l'intégrité des informations de la SAQ afin de les protéger contre les risques et incidents.

« **Utilisateurs** » : Ensemble des individus (employés, gestionnaires, administrateurs, fournisseurs, partenaires d'affaires, etc.) qui accèdent aux informations détenues par la SAQ.

3. PORTÉE

La présente Politique s'applique :

- À tout utilisateur qui crée, collecte, consulte, utilise, sauvegarde, communique ou transporte et supprime les informations détenues par la SAQ;
- Aux informations détenues par la SAQ, et ce tout au long de leur cycle de vie, peu importe leur forme, leur support, leur dispositif, leur emplacement ou le moyen de communication utilisé pour les transiter et peu importe si leur conservation est assurée par elle-même ou par un tiers.

Le non-respect de cette Politique par un utilisateur peut entraîner des sanctions pouvant aller jusqu'au congédiement ou à la résiliation de contrat.

4. DOCUMENTS DÉCOULANT DE LA PRÉSENTE POLITIQUE

Directives : Établissent les règles permettant la mise en œuvre des orientations et principes directeurs de la Politique.

Procédures : Expliquent les étapes à suivre pour atteindre les objectifs fixés par les politiques et directives.

5. PRINCIPES DIRECTEURS

Les pratiques en matière de sécurité de l'information au sein de la SAQ doivent être éthiques, adaptées et réévaluées périodiquement en tenant compte des bonnes pratiques et du risque associé pour les informations à protéger.

La SAQ mise sur un programme de formation et de sensibilisation afin de responsabiliser et d'encourager le développement de bonnes pratiques en matière de sécurité de l'information auprès des utilisateurs.

La SAQ exerce, en conformité avec la législation en vigueur, des activités de surveillance en continu sur tout usage de ses informations et de ses systèmes informatiques. Des contrôles sont réalisés pour favoriser l'efficience opérationnelle des activités de sécurité, détecter et gérer les vulnérabilités et d'éventuels incidents.

6. RÔLES ET RESPONSABILITÉS

La SAQ attribue des rôles et responsabilités à tous les utilisateurs prenant part au cycle de vie de ses informations afin de supporter adéquatement ses affaires et permettre la reddition des comptes.

Conseil d'administration

- Approuver la présente Politique, le programme de protection des informations et de cybersécurité de la SAQ et les niveaux de risque acceptables liés aux menaces à la sécurité de l'information;
- Prendre acte des enjeux importants mettant à risque la sécurité des informations de la SAQ et statuer sur les recommandations qui lui sont présentées.

Comité d'audit

- Analyser les principaux risques en matière de protection de l'information et de cybersécurité auxquels la SAQ s'expose et examiner les mesures prises par la direction pour surveiller et contrôler ces risques;
- Recevoir des rapports réguliers sur les incidents, les impacts opérationnels et les mesures prises pour les résoudre.

Comité de direction

- Déterminer les orientations en matière de sécurité de l'information et les niveaux de risques acceptables pour l'entreprise;
- Approuver les directives en matière de sécurité de l'information, la liste des propriétaires et le niveau de criticité des informations;
- Approuver le programme de protection des informations et de cybersécurité de la SAQ et en faire la recommandation au comité d'audit et au conseil d'administration;
- Analyser les bilans en matière de sécurité de l'information et faire des rapports réguliers au comité d'audit sur les incidents, les impacts opérationnels et les mesures prises pour les résoudre;
- S'assurer de la préparation de l'organisation en vue d'un incident majeur;
- Fait rapport au comité d'audit et au conseil d'administration notamment des enjeux pouvant mettre à risque les informations de la SAQ.

Vice-présidence aux technologies de l'information

- S'assurer de la mise en place et du respect des règles d'utilisation des outils technologiques;
- Analyser les risques identifiés par le CISO et élaborer les plans de mitigation TI.

Directeur de la sécurité de l'information (CISO) :

- Concevoir les politiques, directives et procédures de sécurité de l'information et les maintenir à jour;
- Élaborer le programme de sécurité de l'information, contribuer à la classification de l'information et s'assurer de l'effectivité des contrôles;
- Coordonner l'architecture de la sécurité de l'information et assurer l'arrimage des choix organisationnels, contractuels et technologiques pouvant l'impacter;
- Étudier et approuver toute demande de dérogation ou d'exception aux directives et procédures découlant de la Politique;
- Identifier les risques liés à la sécurité de l'information, proposer les lignes directrices des plans de mitigation opérationnels et en effectuer la reddition de comptes auprès de la haute direction;
- Au besoin, conseiller la haute direction sur le niveau de criticité adéquat ainsi que la nomination des propriétaires pertinents pour les informations critiques;
- Assurer le respect des règles de sécurité lors du partage d'information à l'interne ou avec des tiers;
- Prendre en charge et coordonner la gestion des incidents de sécurité majeurs;
- Planifier et déployer le programme de formation et de sensibilisation en cybersécurité.

Responsable de la protection des renseignements personnels

- S'assurer du respect et de la mise en œuvre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* au sein de la SAQ;
- Diriger le comité de l'accès à l'information et de la protection des renseignements personnels.

Comité de l'accès à l'information et de la protection des renseignements personnels

- Analyser, émettre des directives et réviser toutes les questions ayant trait à la collecte et la protection des renseignements personnels.

Propriétaire d'une information critique et/ou comportant des renseignements personnels

- En collaboration avec le CISO, déterminer le niveau de risque de l'information et les mesures de sécurité adéquates tout au long de son cycle de vie;
- Déterminer les règles de gestion des accès à ses informations, s'assurer de leur respect par les utilisateurs sous sa responsabilité et signaler les incidents de sécurité dont il a connaissance.

Gestionnaires

- Assurer la mise en œuvre et le respect de la présente Politique auprès de leurs équipes et des partenaires d'affaires avec qui ils font affaire;
- S'assurer de la présence des clauses de sécurité dans les contrats ainsi que de leur conformité aux exigences des politiques, directives et procédures de sécurité de l'information;
- Veiller à ce que les utilisateurs sous leurs responsabilités complètent les formations du programme de sensibilisation en cybersécurité;
- Être vigilant et rapporter tout incident de sécurité ou faille potentielle (tout événement suspect, non conforme à la présente politique, brèches de sécurité suspectées ou mauvaise utilisation d'information confidentielle) à leur gestionnaire et au CISO et si des renseignements personnels sont impliqués, au comité sur l'accès à l'information et la protection des renseignements personnels.

Utilisateurs

- Lire, comprendre et se conformer aux politiques, directives et procédures de sécurité de l'information;
- Agir de façon responsable en utilisant les droits d'accès qui leur sont octroyés et en ne les utilisant que pour les tâches attribuées;
- Suivre les formations relatives à la sécurité de l'information;
- Être vigilant et rapporter tout incident de sécurité ou faille potentielle (tout événement suspect, non conforme à la présente Politique, brèches de sécurité suspectées ou mauvaise utilisation d'information confidentielle) à son gestionnaire et au CISO.

7. GOUVERNANCE DE LA POLITIQUE

La présente Politique est sous la responsabilité de la Vice-présidence des technologies de l'information et entre en vigueur dès son approbation par le conseil d'administration.

Le CISO est chargé d'en faire une révision annuelle et de soumettre tout changement pour approbation au comité de direction, comité d'audit et au conseil d'administration.