SAQ

POLITIQUE

No : 023 150 013 02

Rédigée par : Division des technologies de l'information	**Section :**	GESTION DES TECHNOLOGIES DE L'INFORMATION	**Émetteur :** Technologies de l'information
	Sous-section :	GESTION DES RISQUES ET SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION	
	Sujet :	Politique générale de la sécurité de l'information	**Adoptée par le Conseil d'administration :** 29 mai 2008 **Refondue :** 26 mars 2021

1. CONTEXTE

- La Société des alcools du Québec (ci-après « SAQ ») a adopté une politique générale de la sécurité de l'information qui permet à la SAQ, compte tenu de l'importance d'assurer une bonne protection des actifs informationnels et des renseignements confidentiels, de doter l'organisation d'un cadre de sécurité de l'information.

- La politique vise la protection de l'information tout au long de son cycle de vie, en assurant sa confidentialité, son intégrité, sa disponibilité et sa destruction au moment opportun.

- Elle *est adoptée dans le respect des lois auxquelles la SAQ est assujettie notamment à la Loi sur l'accès aux documents des organismes publics* et sur la protection des renseignements personnels, ainsi que la *Loi sur les archives*. Elle assure aussi le respect des exigences contenues dans la norme de sécurité de l'industrie des cartes de paiements (norme PCI-DSS).

2. OBJECTIF

La présente politique a pour objectif d'établir les rôles et responsabilités de tous les utilisateurs ayant accès à des actifs informationnels appartenant à la SAQ afin de favoriser une meilleure sécurité de l'information.

Les règles générales de conduite en matière de sécurité de l'information et les attentes quant à l'application de mesures et de contrôles de sécurité des actifs informationnels de la SAQ sont établies en fonction des priorités d'affaires de la SAQ, de l'importance des actifs à protéger, qu'ils soient critiques ou non, des impératifs de rentabilité, de leur confidentialité, des risques inhérents à la situation et des lois et règlements auxquels la SAQ est assujettie.

Pour favoriser la sécurité de l'information, des processus, mesures et contrôles de sécurité sont mis en place. Ces contrôles favorisent l'efficience opérationnelle des activités de sécurité, en tenant compte des coûts pour l'ensemble des intervenants impliqués.

La SAQ instaure cette politique en respect avec les règles de sécurité de l'information suivantes :

Protection de l'information

Afin de protéger l'information qu'elle détient, la SAQ réalise les activités suivantes:

- Mise à jour de l'inventaire des principaux actifs informationnels et identification des actifs critiques devant faire l'objet de protection accrue;
- Désignation d'un responsable pour tout actif informationnel critique ou qui contient des renseignements personnels.
- Sécurité physique adéquate pour protéger les informations et les équipements;
- Sécurité logique adéquate pour protéger les informations et les équipements tels que : configuration des paramètres de sécurité, paramètres des mots de passe, journalisation et alertes;
- Vérification des antécédents judiciaires pour tous les employés de la SAQ incluant les personnes ayant accès à des actifs informationnels critiques;
- Conditions d'emploi spécifiant la responsabilité de l'employé en matière de sécurité de l'information;
- Contrôle des accès par la personne responsable des actifs informationnels et les TI;
- Formation appropriée aux utilisateurs en fonction des risques et impacts de bris de sécurité;
- Gestion sécuritaire des technologies de l'information par exemple, par la mise en place de rustines, pare-feu, etc.;
- Destruction de l'information de manière sécuritaire en temps opportun.

Protection des informations confidentielles

L'information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée ou illicite. Toutefois, en conformité avec les dispositions de la *Loi facilitant la divulgation d'actes répréhensibles* à l'égard des organismes publics, ceci n'a pas pour but de dissuader la communication d'information dans le but de mettre en lumière des actes répréhensibles à l'égard de la SAQ.

Sont considérés comme confidentiels, les renseignements personnels ainsi que toute information de nature commerciale dont la divulgation aurait des incidences néfastes pour la SAQ, ses partenaires, client ou fournisseurs, ainsi que sur les résultats financiers de la SAQ. L'information pour laquelle la SAQ s'est engagée contractuellement à protéger ou qui constitue une information concurrentielle importante pour ses fournisseurs et partenaires doit également être traitée de façon confidentielle.

Surveillance des activités

La SAQ exerce, en conformité avec la législation et la règlementation en vigueur, des activités de surveillance sur tout usage de ses actifs informationnels et de ses systèmes informatiques.

3. PORTÉE

La présente politique s'applique à tous les administrateurs, gestionnaires, employés, fournisseurs, partenaires d'affaires, clients ou toutes autres personnes qui consultent, utilisent, sauvegardent, transportent ou communiquent les actifs informationnels de la SAQ.

Cette politique vise tout actif informationnel de la SAQ, et ce, tout au long de son cycle de vie, peu importe sa forme, son support, son emplacement ou le moyen de communication utilisé pour le transiter et peu importe si la conservation est assurée par elle-même ou par un tiers. Pour plus de précision et sans limiter ce qui précède, sont visés à titre d'exemple différents supports tangibles et intangibles permettant le traitement, la transmission ou la conservation de l'actif informationnel : papier, logiciel, base de données, réseau, vidéos ou enregistrement verbal.

La conformité à la politique est obligatoire et peut être sujette à des contrôles de suivi et de surveillance.

4. RÔLES ET RESPONSABILITÉS

Conseil d'administration

Le conseil d'administration a la responsabilité :

- d'approuver la présente politique;
- d'approuver le programme de protection des actifs informationnels y compris la cybersécurité de la SAQ et d'en faire un suivi rigoureux;
- de prendre acte des enjeux importants mettant à risque la sécurité des actifs informationnels de la SAQ;
- de prendre connaissance, d'analyser, d'émettre des recommandations ou de prendre des décisions à l'égard des bilans soumis à son attention.

Comité de direction

Le Comité de direction a la responsabilité :

- de déterminer les orientations portant sur les principes de sécurité de l'information, incluant son programme de cybersécurité et d'en assurer le suivi de ses actions;
- d'approuver les directives et standards applicables en matière de sécurité des actifs informationnels;

- d'approuver la liste des propriétaires et le niveau de criticité pour les actifs informationnels comportant des renseignements personnels;
- de soumettre et de recommander au conseil d'administration tous les dossiers qui concernent la sécurité et qui requièrent l'attention de celui-ci.

Vice-présidence aux technologies de l'information

La vice-présidence aux technologies de l'information est responsable :

- de conseiller et de recommander à la haute direction en matière de sécurité selon les risques potentiels pour la SAQ ainsi que leurs stratégies d'atténuation;
- de conseiller et de recommander au comité de l'accès à l'information et au comité de direction sur le niveau de criticité ainsi que sur les propriétaires ciblés pour les actifs informationnels critiques;
- de conseiller les propriétaires d'actifs informationnels sur les bonnes pratiques instaurées à la SAQ pour assurer la protection de la donnée;
- de mettre en place des mesures de sécurité telles que définies dans son programme de cybersécurité et d'en assurer leurs surveillances;
- de s'assurer de la mise en place et du respect d'une saine gestion des risques et de la sécurité de l'information au sein de la SAQ.
- de s'assurer de la mise en place et du respect des règles d'utilisation des outils technologiques.

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

Le Comité de l'accès à l'information et de la protection des renseignements personnels est chargé d'accomplir les fonctions énoncées dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, notamment, il doit :

- s'assurer de la mise en place des bonnes pratiques en matière de protection de renseignements personnels au sein de la Société;
- établir un niveau de criticité et les propriétaires pour les actifs informationnels comportant des renseignements personnels;
- réviser les questions relatives à la protection de la vie privée des systèmes d'information et proposer des directives pour la protection des renseignements personnels, notamment pour la conservation des données par des tiers et à l'extérieur du territoire du Québec;
- approuver les analyses de sécurité liées à la protection des renseignements personnels des projets informatiques;
- informer la vice-présidence aux technologies de l'information et le Comité de direction de toute situation pouvant compromettre la sécurité des renseignements personnels;

Propriétaire d'un actif informationnel critique ou d'un actif informationnel comportant des renseignements personnels

Le propriétaire d'un actif informationnel est responsable de :

- s'assurer que l'actif informationnel pour lequel il a été désigné propriétaire est classé de façon à encadrer adéquatement son utilisation, son traitement, son entreposage, sa distribution, sa destruction et sa protection. Les contrôles mis en place doivent tenir compte des supports sur lesquels l'information est entreposée, des plateformes technologiques utilisées et des méthodes pour la diffuser. Cette responsabilité est soutenue par la cartographie de données réalisée en collaboration entre les TI et le propriétaire de la donnée.
- s'assurer que pour l'actif informationnel pour lequel il a été désigné propriétaire que seules les données personnelles nécessaires à l'exercice des fonctions dudit actif sont recueillies.
- s'assurer que l'actif informationnel pour lequel il a été désigné propriétaire est accessible uniquement par les systèmes et les personnes autorisées. Cette responsabilité est soutenue par le processus de gestion des accès.
- de rapporter tout incident de sécurité ou faille potentielle impliquant l'actif informationnel pour lequel il a été désigné propriétaire à la vice-présidence aux technologies de l'information et au comité sur l'accès à l'information et la protection des renseignements personnels si des renseignements personnels sont impliqués;
- de faire appliquer les normes et directives émises à l'égard de la protection des actifs informationnels pour les actifs dont il a été désigné propriétaire.

Gestionnaires

Les gestionnaires de la SAQ sont responsables de :

- la mise en œuvre auprès de leurs employés, de leurs partenaires d'affaires et fournisseurs avec qui ils font affaire, des dispositions de la présente politique;
- s'assurer que les contrats signés avec des tiers comportent des clauses portant sur les dispositions de la présente politique;
- veiller à ce que les personnes qui détiennent des accès appliquent les mesures de protection requises pour assurer la sécurité dudit actif, le tout encadré par la directive sur l'utilisation des technologies;
- veiller à ce que les personnes sous sa responsabilité effectuent toutes les formations soumises par le programme de sensibilisation en cybersécurité;
- de rapporter tout incident de sécurité ou faille potentielle à la vice-présidence aux technologies de l'information et au comité sur l'accès à l'information et la protection des renseignements personnels si des renseignements personnels sont impliqués.

Utilisateurs

Les utilisateurs de la SAQ sont responsables de :

- se conformer à la présente politique et à ses directives d'application, et ce, que l'utilisation du matériel mis à leur disposition ou la consultation des données se fasse dans les locaux de la SAQ ou à l'extérieur de ceux-ci.
- protéger l'information à laquelle ils ont accès, et utiliser les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès autorisés. L'utilisateur ne doit accéder qu'aux informations nécessaires à son travail, même s'il dispose d'accès plus larges. Ainsi, il est interdit aux utilisateurs à hauts privilèges d'abuser de leur privilège en accédant à des informations qui ne leur sont pas destinées et qui ne supportent pas leurs tâches.
- d'assumer l'entière responsabilité de toute action qu'ils auront effectuée avec leur compte. Pour ce, l'accès aux services informatisés de la SAQ est contrôlé par un identifiant personnel et une authentification par mot de passe. L'utilisateur ne doit pas partager avec d'autres utilisateurs son identifiant personnel (code d'utilisateur) et son mot de passe. L'utilisateur doit obligatoirement effectuer toutes les formations soumises à cet égard par le programme de sensibilisation en cybersécurité.
- l'utilisateur reconnaît que la SAQ peut exercer un contrôle de l'utilisation des actifs informationnels dans les limites de la législation et la règlementation en vigueur et qu'il ne dispose pas de garantie de confidentialité dans ses communications électroniques.
- de rapporter tout incident de sécurité ou faille potentielle impliquant l'actif informationnel (tout événement non conforme à la présente politique, brèches de sécurité suspectées ou mauvaise utilisation d'information confidentielle) à son gestionnaire et à la vice-présidence aux technologies de l'information;

Tout logiciel, solution infonuagique ou appareil mobile doit être approuvé et, le cas échéant, installé par le personnel de la division TI afin d'assurer le respect des exigences de sécurité de la SAQ. Dans un contexte ou l'utilisation d'un appareil mobile personnel est requise, seule la suite des outils bureautiques déterminée est autorisée pour accéder aux fichiers de la SAQ. Toutefois, dans le cas des membres du conseil d'administration de la SAQ, l'usage d'appareils n'appartenant pas à la SAQ est autorisé. L'administrateur qui consulte des fichiers concernant la SAQ doit prendre les mesures appropriées et raisonnables pour assurer la confidentialité de ceux-ci et doit s'assurer de leur destruction lorsqu'ils ne sont plus nécessaires à leurs fonctions.

Les utilisateurs qui ne se conforment pas à cette politique s'exposent à des mesures disciplinaires, administratives ou légales en fonction de la gravité de leur geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, cessation de la relation d'affaires, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

5. DÉFINITIONS

Dans la présente politique, on entend par :

« **Utilisateurs** », l'ensemble des individus (employés, gestionnaires, administrateurs, fournisseurs, partenaires d'affaires, etc.) qui accèdent à des actifs informationnels appartenant à la SAQ.

« Actif informationnel », l'ensemble des données ou des informations, peu importe sa forme, son support ou son emplacement, appartenant à la SAQ.

« Actif informationnel critique », l'ensemble des données ou des informations qui nécessitent une disponibilité contrôlée, une grande intégrité et qui possèdent un niveau de confidentialité élevé.

« Renseignements personnels », tout renseignement qui concerne une personne physique et qui permet de l'identifier.

« **Confidentialité** », propriété d'une information de n'être accessible qu'aux personnes ou entités désignées ou autorisées.

6. GOUVERNANCE DE LA POLITIQUE

La présente politique entre en vigueur dès son approbation par le conseil d'administration.

La vice-présidence aux technologies de l'information est chargée de la révision annuelle de la présente politique. Lorsque requis, les modifications seront présentées pour approbation.