POLITIQUE GÉNÉRALE DE LA SÉCURITÉ DE L'INFORMATION

Adoptée par le conseil d'administration du 1er juin 2017 [CA 2017-05-033.05]

INTRODUCTION

La Société des alcools du Québec, ci-après appelée la «SAQ», expose ici sa politique générale de la sécurité de l'information.

Cette politique a pour but de faire connaître à ses clients, ses employés, ses fournisseurs et ses partenaires d'affaires (ci-après « les utilisateurs ») les responsabilités de chacun à l'égard du cadre de sécurité mis en place par la SAQ pour l'information qu'elle détient, quel que soit son support ou son moyen de communication et qu'importe si la conservation est assurée par elle-même ou par un tiers.

Cette 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).

1. CADRE ET PORTÉE

La présente politique et les directives de sécurité s'y rattachant s'appliquent à tous les employés, fournisseurs et partenaires d'affaires de la SAQ qui utilisent, sauvegardent, transportent ou communiquent les actifs informationnels de la SAQ ainsi qu'à toute personne en mesure d'y avoir accès. Les actifs informationnels incluent l'information ainsi que les supports tangibles et intangibles (ex. : papier, matériel, logiciel, réseau, vidéos, enregistrement verbal) permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue.

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

2. OBJECTIFS

Les objectifs de cette politique sont d'édicter les règles générales de conduite en matière de sécurité de l'information et de définir les attentes quant à l'application de mesures et de contrôles de sécurité des actifs informationnels de la SAQ. Elles 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 atteindre ces objectifs, les processus, mesures et contrôles de sécurité visent à minimiser les risques pour les actifs informationnels de la SAQ afin d'en assurer la confidentialité, l'intégrité, la disponibilité et la destruction en temps opportun. Elle favorise l'efficience opérationnelle des activités de sécurité, au moindre coût possible pour l'ensemble des intervenants impliqués.

3. RÔLES ET RESPONSABILITÉS

3.1 Propriétaire d'un actif informationnel critique

Le propriétaire d'un actif informationnel critique désigné par le comité de direction de la SAQ est responsable de s'assurer que :

- chaque actif informationnel critique 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.

- les critères définissant l'accès à cet actif assurent la restriction sur la base du besoin d'affaires, établi en fonction des tâches à accomplir dans le cadre des fonctions attribuées. L'utilisation des informations doit être restreinte aux fins pour lesquelles elles ont été destinées.

- une évaluation du risque de sécurité est effectuée pour déterminer si les mesures de contrôles sont suffisantes compte tenu des impacts potentiels pour la SAQ. Cette évaluation est effectuée en collaboration avec les experts TI. La personne qui accepte un risque est imputable des impacts encourus par ce risque.

- un plan de formation adéquat sur la protection des informations est transmis aux gestionnaires à l'intention des employés concernés, lequel doit indiquer la fréquence de la sensibilisation.

Le transfert ou la délégation de tâches à un tiers pour la gestion d'un actif informationnel ne change pas la responsabilité du propriétaire de cet actif.

3.2 Gestionnaires

Les gestionnaires sont responsables de la mise en œuvre auprès de leurs employés, des partenaires et fournisseurs avec qui ils font affaire, des dispositions de la présente politique et de ses directives d'application.

3.3 Utilisateurs

Les utilisateurs doivent se conformer à la présente politique et à ses directives d'application. Ils doivent 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 haut privilèges d'abuser de leur privilège en accédant à des informations qui ne leur sont pas destinées et qui ne supportent pas leurs tâches.

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 permettre à d'autres d'avoir accès à ces services au moyen de son identifiant personnel. L'utilisateur assume l'entière responsabilité de toute action liée à son compte.

L'utilisateur reconnaît qu'il ne dispose pas de garantie de confidentialité dans ses communications électroniques.

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.

Il incombe à toutes les ressources de la SAQ de communiquer avec son gestionnaire ou l'équipe de sécurité TI tout événement non conforme à la présente politique, brèches de sécurité suspectées ou mauvaise utilisation d'information confidentielle.

4. RÈGLES DE SÉCURITÉ DE L'INFORMATION

La présente section décrit les règles en matière de sécurité de l'information.

4.1. Protection de l'information

Les actifs informationnels doivent être protégés en fonction des priorités d'affaires de la SAQ, de l'importance des actifs à protéger, des impératifs de rentabilité, de leur confidentialité, des risques inhérents à la situation et des lois et règlements auxquels la SAQ est assujettie. Cette protection s'appuie sur les mesures 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;
- Sécurité physique adéquate pour protéger les informations et les équipements;
- Sécurité logique adéquate pour protéger les informations et les équipements telle que : configuration des paramètres de sécurité, paramètres des mots de passe, journalisation et l'alertage;
- Vérification des antécédents pour les personnes ayant accès à des actifs informationnels critiques
- Les conditions d'emploi stipulent 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.

4.2. 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 concernant les partenaires, clients et fournisseurs dont la divulgation aurait des incidences néfastes, notamment sur la réputation de la SAQ ainsi que ses résultats financiers. L'information pour laquelle la SAQ s'est engagée contractuellement à protéger ou qui constitue une information concurrentielle importante pour nos fournisseurs et partenaires doit également être traitée de façon confidentielle.

4.3. Surveillance des activités

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

5. SANCTIONS

Les employés, fournisseurs ou partenaires d'affaires sont tenus de se conformer à la présente politique et aux directives et instructions qui en découlent et qui leur sont communiquées par leur gestionnaire ou autre personne en autorité. Si une de ces personnes ne se conforme pas à cette obligation, elle s'expose à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son 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.

6. GOUVERNANCE DE LA POLITIQUE

Chaque vice-président est responsable de l'application de cette politique pour les actifs informationnels qui relèvent de sa direction.

Le vice-président TI est responsable de la mise en place des mesures de sécurité et de leur surveillance, selon le niveau de sécurité établi de concert avec les propriétaires des actifs informationnels. Il conseille la haute direction sur les risques potentiels en matière de sécurité de même que sur les stratégies d'atténuation de ceux-ci. De plus, il recommande à la haute direction les orientations stratégiques et les priorités d'intervention en matière de sécurité des actifs informationnels. Il assure la vigie des nouveaux risques en matière de sécurité technologique. Le vice-président TI est aussi responsable d'effectuer la mise à jour de cette politique annuellement ou lorsque des changements importants surviennent.