Place des Arts
Québec

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION ET LA CYBERSÉCURITÉ

Avril 2018

Adoptée : Rés. CA 2018-13

TABLE DES MATIÈRES

1. OBJET

La poursuite des activités de la Société de la Place des Arts de Montréal (ci-après « la Société ») repose sur un ensemble de systèmes d'informations composés de logiciels, d'applications et d'infrastructures technologiques. Ces systèmes communiquent, stockent et traitent en permanence des informations.

L'objet de la présente Politique de sécurité (la « Politique ») est de mettre en place une gestion efficace de la sécurité de l'information et de la cybersécurité au sein de l'organisation, et plus particulièrement de :

- Permettre la mise en œuvre, le maintien et la mise à disposition d'informations accessibles au besoin, fiables, intègres, dignes de confiance et dans certains cas, d'en préserver la confidentialité;
- Maximiser la valeur de l'information et des actifs informationnels en améliorant leur utilisation de manière sécuritaire;
- Promouvoir la sécurité de l'information et la cybersécurité, ce qui constitue un ensemble de bonnes pratiques d'affaires, incluant la protection des données de titulaires de cartes de crédit et leurs renseignements personnels, la sécurité des applications, la sécurité du réseau, la protection des actifs informationnels et l'utilisation sécuritaire des technologies de l'information.

2. PORTÉE ET OBJECTIFS

La Politique établit les orientations de la Société en matière de sécurité de l'information et de cybersécurité. Elle définit les principes de sécurité qui lui sont propres et fixe les objectifs et les conditions préalables à la mise en œuvre des mesures de sécurité considérées comme essentielles à la sécurité de son information.

Elle complète les différentes actions de sécurité de l'information déjà menées et s'appuie sur les diverses composantes du Cadre de gouvernance identifiées à l'Annexe A.

La présente Politique s'applique aux utilisateurs, aux informations que la Société stocke, traite ou transige, les processus de gestion et les technologies utilisées et les risques auxquels le tout est exposé.

Plus spécifiquement, elle s'applique aux :

- **Utilisateurs** : pour informer le personnel, les fournisseurs de services et tous ceux qui interviennent pour le compte de la Société, des comportements attendus et des mesures de sécurité applicables pour protéger les informations et les actifs informationnels de la Société.
- **Informations** : pour évaluer adéquatement la sensibilité de l'information détenue ou utilisée par la Société dans le cadre de ses opérations, peu importe sa nature, sa localisation et le support sur lequel elle se trouve, et ce, durant tout son cycle de vie. Elle concerne également l'information confiée à des tiers et toute forme d'échange, y compris les services en ligne et les actifs informationnels supportant l'ensemble de ces informations.
- **Processus de gestion** : pour gérer efficacement et de manière sécuritaire ainsi que pour protéger l'information et les actifs informationnels sensibles.
- **Technologies** : pour identifier le niveau de protection approprié à l'égard des technologies et des actifs informationnels existants ou à venir et définir les raisons de le faire et ce, le cas échéant, dès l'étape de conception d'un processus ou d'un système d'information, lors de l'élaboration d'une entente ou de l'acquisition d'une solution technologique.
- **Risques** : pour gérer efficacement les risques liés à la sécurité de l'information et leurs mesures d'atténuation tout au long du cycle de vie de l'information et de l'actif informationnel.

La Politique a pour objectif de servir de cadre de référence aux orientations de sécurité de l'information et de cybersécurité de la Société et aux comportements attendus.

Elle vise à établir une vision et une compréhension commune des enjeux, des mesures et des comportements attendus en sécurité de l'information et cybersécurité au sein de l'organisation, au travers notamment les directives de sécurité afférentes.

Plus spécifiquement, la présente politique vise les objectifs suivants :

- Soutenir la mission de la Société;
- Assurer le respect de la vie privée des citoyens et employés, notamment la confidentialité des renseignements personnels et la sécurité des données des titulaires de cartes de crédit;
- Promouvoir un comportement responsable.

3. PRINCIPES DE SÉCURITÉ

La sécurité de l'information et la cybersécurité sont essentielles pour la Société et représentent un enjeu important. Elles supportent sa mission et ses opérations tout en faisant la promotion d'une culture responsable de la sécurité par l'application des principes directeurs suivants :

- **Mettre l'accent sur les activités de base :** la sécurité de l'information doit être intégrée à l'ensemble des activités de base et plus particulièrement, celles qui lui sont essentielles. Ce faisant, la Société peut optimiser ses ressources et supporter les exigences de sécurité liées à sa mission et à ses besoins. Elle protège ainsi ses processus essentiels contre des incidents de sécurité ayant un impact significatif. Toutefois, la sécurité de l'information ne doit pas se faire au détriment du bon déroulement des activités.
- **Assurer la sécurité de l'information :** protéger l'information contre toute atteinte à sa disponibilité, son intégrité ou sa confidentialité susceptible de causer des dommages à la Société, aux entreprises, aux citoyens ou à ses partenaires.
- **Renforcer la confiance de toutes les parties prenantes :** en leur permettant d'avoir accès aux informations requises dans l'exercice de leur fonction.
- **S'adapter aux menaces et aux risques** : protéger l'information en fonction de sa valeur et des risques auxquelles elle est exposée. Il est nécessaire d'évaluer les menaces actuelles et futures de manière continue afin de permettre une prise de décision éclairée et des actions adéquates pour atténuer les risques de manière efficace. Réviser périodiquement les directives et les mesures de protection et de sécurité qui en découlent afin de tenir compte des menaces, des risques ainsi que des changements organisationnels et technologiques.
- **Se conformer aux exigences juridiques et réglementaires :** pour s'assurer de respecter les obligations applicables et éviter toutes conséquences défavorables découlant de leur non-respect.
- **Promouvoir l'approche d'amélioration continue :** pour réduire les coûts, créer de la valeur, optimiser les ressources et améliorer l'efficacité et l'efficience des mesures de sécurité. Pour fournir au besoin et en temps voulu des indicateurs sur la performance de la sécurité de l'information.
- **Agir de manière éthique, professionnelle et promouvoir une culture de sécurité positive et responsable :** pour partager la préoccupation à l'égard de la sécurité de l'information avec l'ensemble du personnel, des fournisseurs et des partenaires. Pour influencer positivement les comportements des utilisateurs, réduire la probabilité d'incident et en limiter les impacts éventuels par une culture éclairée (utilisateurs conscients et informés), juste (utilisateurs responsables), formatrice (utilisateurs encouragés à faire part de leurs besoins et à améliorer leurs connaissances et leurs compétences). La formation et la sensibilisation à l'égard de la sécurité de l'information sont essentielles et exigent une démarche continue.

4. STRUCTURE ORGANISATIONNELLE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION ET DE LA CYBERSÉCURITÉ

Pour implanter et supporter la présente politique et les documents afférents, les responsabilités suivantes s'appliquent :

- **Conseil d'administration (CA) :** Considérant que la sécurité de l'information est un élément essentiel pour la mission de la Société, le CA porte la responsabilité finale concernant tous les aspects de la sécurité, incluant celle de la sécurité de l'information.
- **Président-directeur général (PDG) :** Le PDG supervise les activités stratégiques essentielles à la sécurité informatique. Il a la responsabilité de présenter, le cas échéant, toute information pertinente pour le CA concernant la sécurité informatique de la Société.
- **Comité de direction de la Société (CD) :** Le CD appuie le PDG dans son rôle de protection et de sécurité de l'information. Il a la responsabilité globale de s'assurer, au travers d'un suivi et d'un examen périodique, que les bonnes pratiques en sécurité de l'information sont appliquées de manière efficace et cohérente au sein de l'organisation.
- **Directeur, Finances et Administration (DFA) :** Le DFA supervise les activités tactiques reliées à la sécurité des technologies de l'information. Il a la responsabilité de présenter au CD les politiques et autres documents ou enjeux pertinents, en temps opportun, pour discussion et/ou décision.
- **Mandataires / Détenteur de l'Information :** Les mandataires / détenteurs de l'information sont les gestionnaires désignés comme responsable d'un ou plusieurs actifs informationnels. Ils agissent à titre de responsable de la sécurité de l'information des actifs informationnels sous leur responsabilité et s'assurent que les ressources qui les supportent sont bien sécurisées. Pour ce faire, ils approuvent les risques résiduels auxquels leurs actifs restent exposés.
- **Responsable de la Sécurité de l'Information :** le RSI a la responsabilité d'une part de concevoir et réaliser le programme de la sécurité de l'information, incluant la mise en œuvre et la révision de cette Politique et des documents s'y rattachant, et d'autre part de prendre les décisions pour évaluer, contrôler, optimiser, financer et suivre les risques quels qu'ils soient, dans le but de générer de la valeur ajoutée à court ou à long terme. Il fournit à la haute direction, l'assurance complète que la sécurité de l'information est conforme aux besoins, en se basant sur le plus haut niveau d'objectivité et d'indépendance possible.

  Au sein de la Société, le RSI est aussi responsable de la bonne gestion des ressources, des solutions et des mesures de sécurité de l'information et de cybersécurité. Il prendra toutes les mesures jugées nécessaires afin d'assurer la protection de l'infrastructure et de l'information de la Société, incluant l'application et le respect des directives de sécurité. Ces mesures peuvent comprendre notamment, mais sans s'y restreindre :

  - Le contrôle (autoriser / bloquer) des flux de communication entrant ou sortant de l'organisation ou transitant au sein de la Société;
  - L'inspection automatisée ou manuelle du trafic chiffré et non chiffré transitant sur le réseau corporatif (courriels, dépôt de documents dans l'infonuagique, etc.);
  - L'inspection de tous les éléments (courriels, fichiers, exécutables, plug-in, macros, etc.) présents sur le réseau de la Société;
  - Des balayages antivirus pour vérifier qu'il n'y a pas d'applications ou de vulnérabilités mettant en péril la sécurité de l'information de manière « ad hoc »;
  - Des tests d'intrusion afin de confirmer l'efficacité des mesures de sécurité en place;
  - Pour un motif de sécurité raisonnable, déconnecter, exclure du réseau ou saisir un poste utilisateur afin d'assurer une réponse aux incidents de sécurité efficiente;

- S'assurer, par moyen automatisé ou manuel, qu'il n'y a pas de fuite d'informations sensibles par l'entremise des technologies de l'information;
- Collecter des journaux d'utilisation des TI conformément à la Directive « journalisation des événements de sécurité »;
- Imposer un moratoire de trente (30) jours à l'introduction ou l'exploitation d'un nouveau logiciel ou équipement en production qui pourrait constituer une menace de sécurité en attendant un avis et une évaluation de sécurité;
- Enquêter sur les événements menant à un incident de sécurité afin d'établir l'ampleur de l'incident.

- **L'utilisateur :** Les employés, les sous-traitants et toutes autres personnes dûment autorisées sont considérés comme des utilisateurs. Les utilisateurs ont la responsabilité d'agir en tout temps dans le respect de cette Politique.

5. DISPOSITIONS FINALES

5.1 Révision, validation et approbation

Une révision complète de cette Politique doit être faite selon un calendrier défini par le responsable de la sécurité de l'information.

Cette révision doit être validée par le CD et approuvée ensuite par le PDG et le CA.

5.2 Surveillance, performance, suivi et audit.

Le responsable de la sécurité de l'information, en collaboration avec le DFA, s'assurera de l'application de la présente Politique et indiquera si ses objectifs ont été satisfaits et si des suivis s'avèrent nécessaires. Le cas échéant, le DFA fera rapport au CD.

L'application de cette Politique doit faire l'objet d'une vérification par audit interne ou externe, au minimum tous les trois (3) ans.

5.3 Exceptions et exemptions

Il n'existe aucune exception possible à la présente Politique.

Toutefois, des exemptions à son application sont possibles. Elles seront consignées dans un registre approuvé par le DFA.

5.4 Distribution et affichage

Cette Politique est publiée sur l'intranet et sur le site Internet de la Société.

5.5 Autorisation

Cette politique a été approuvée par conseil d'administration le 23 avril 2018 par la résolution CA 2018-13

6. RÉFÉRENCES CONNEXES

Cette Politique s'inscrit dans le Cadre de Gestion de la Sécurité de l'Information et de la Cybersécurité, lequel décrit spécifiquement la mise en œuvre des mécanismes de concertation en sécurité de l'information, c'est-à-dire les rôles et les responsabilités de toutes les parties prenantes, incluant leurs mandats et autorité associés.

La Société veille également à se conformer aux lois et règlements applicables à la sécurité de l'information ainsi qu'aux normes de l'industrie. Pour tout complément d'information, vous référer au Cadre juridique et normatif.

Enfin, cette Politique se traduit en diverses Directives de sécurité, traitant chacune d'une thématique spécifique.

L'ensemble de ces documents font partie de la présente Politique et constitue le Cadre de gouvernance de la sécurité de l'information et de la cybersécurité de la Société, tel que représenté en Annexe A.

7. HISTORIQUE DES VERSIONS

Version Nº	Date	Révisée par	Autorisée par
1			

ANNEXE A

CADRE DE GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION ET DE LA CYBERSÉCURITÉ