Politique sur la sécurité de l'information de la SHDM

Adoptée par les membres du conseil d'administration
le 29 mai 2018

Direction générale
Bureau des technologies de l'information

Adoptée le 29 mai 2018 (résolution 18-040)
Amendée le 30 septembre 2019 (résolution 19-071)
Amendée le 2 novembre 2023 (résolution 23-066)

SHDM

SOCIÉTÉ D'HABITATION
ET DE DÉVELOPPEMENT
DE MONTRÉAL

Table des matières

Préambule

La Politique de sécurité de l'information, ci-après appelée la « Politique », est avant tout la démonstration du soutien et de l'engagement de la Société d'habitation et de développement de Montréal (ci-après « SHDM ») vis-à-vis de la sécurité de l'information et de sa prise de position ferme et claire quant aux mesures de sécurité à appliquer pour protéger ses actifs informationnels. Elle a été élaborée conformément aux obligations légales et administratives et selon les meilleures pratiques. Elle énonce les principes directeurs, identifie les acteurs concernés, précise leurs rôles et responsabilités en lien avec les principes de gestion de la sécurité de l'information.

Section 1

1. Dispositions préliminaires

1.1 Définitions

1.1.1 Dans la Politique, les expressions et les mots suivants signifient :

1. **Actif informationnel** : l'information elle-même ainsi que les systèmes utilisés pour son traitement, son utilisation, son stockage, sa conservation, sa destruction et sa communication interne et externe.

2. **Cycle de vie de l'information** : période correspondant à la durée de vie de l'information, de sa création ou de son acquisition, en passant par son traitement, son stockage, sa transmission, son utilisation, jusqu'à sa restitution, sa destruction ou son archivage, en conformité avec le calendrier de conservation de la SHDM.

3. **Confidentialité** : propriété d'une information de n'être accessible qu'aux personnes désignées et autorisées.

4. **Degré de sensibilité de l'information** : varie selon les informations, sera jugée sensible tout renseignement considéré comme confidentiel, stratégique, essentiel, critique, indispensable ou vital pour les opérations de la SHDM, et dont la divulgation, l'altération, la perte ou la destruction est susceptible de porter préjudice à la SHDM, à son personnel ou à sa clientèle, ses partenaires et ses fournisseurs.

5. **Disponibilité** : propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

6. **Information** : renseignement, quelle que soit la nature de son support et quelle que soit la forme sous laquelle il est accessible, notamment, écrite, graphique, sonore, visuelle. L'information comprend, notamment, les fichiers structurés (bases de données) et non structurés (fichiers Word, Excel, PowerPoint, PDF, etc.), les courriels, les messages texte, les communications et les messages vocaux, les photos, les dessins, les télécopies, les originaux et copies de documents papier, les rapports informatisés ainsi que les copies de sauvegarde et les archives.

7. **Intégrité** : propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

8. **Intervenant** : toute personne physique ou morale ayant un rôle défini à l'article 2.2.13 de la section 2 de la présente Politique ou un tiers (consultants, fournisseurs, partenaires d'affaires) ayant des responsabilités spécifiques en matière de sécurité de l'information.

9. **Système d'information** : inclut tous les serveurs et les clients, l'infrastructure réseau, les systèmes et les logiciels d'application, les données et autres sous-systèmes et composants qui sont détenus ou utilisés par la SHDM ou qui sont sous la responsabilité de cette dernière. L'utilisation d'un système d'information comprend également l'utilisation de tous les services internes ou externes, tels que l'accès Internet, le courriel, etc.

10. **Traçabilité** : propriété d'un document associé à la conservation de tout ce qui le compose, soit sa provenance, de tout changement de support (informatique, papier, audio, visuel, numérique) et la piste des étapes du ou des processus qui ont créé ce document.

11. **Utilisateur** : Tout employé de la SHDM, sans égard à son statut d'emploi, dirigeant, administrateur et membre du conseil ou des comités qui accède ou utilise les Actifs informationnels de la SHDM.

1.2 Objectifs

1.2.1 Les principaux objectifs de la présente Politique sont :

- d'assurer la Disponibilité, l'Intégrité et la Confidentialité de l'information conformément aux lois en vigueur, par l'adoption de politiques, de règlements, de procédures, de directives et de normes au sein de la SHDM;

- de sensibiliser et d'informer les Utilisateurs et les Intervenants quant à leurs rôles et responsabilités dans la protection des Actifs informationnels de la SHDM;

1.3 Champ d'application

1.3.1 Cette Politique s'applique à tous les Intervenants et Utilisateurs de la SHDM.

Les Actifs informationnels visés sont ceux appartenant à la SHDM et exploités par elle, ceux lui appartenant et exploités ou détenus par un fournisseur ou un tiers, ceux appartenant à un fournisseur de services ou un tiers et exploités par lui au profit de la SHDM, ou ceux appartenant à un tiers et détenus par la SHDM.

Toutes les activités impliquant la manipulation, la communication, la conservation, la destruction ou l'utilisation, sous quelle que forme que ce soit des Actifs informationnels, sont touchées par cette Politique.

Section 2

2. Mesures visées par cette Politique

2.1 Principes directeurs

2.1.1 Norme

Les principes de base de la présente Politique s'inspirent de la famille des normes ISO 27000. Ces normes internationales offrent une vue d'ensemble des systèmes de gestion de la sécurité de l'information (SGSI) et édictent des pratiques reconnues afin notamment d'établir ce SGSI.

2.1.2 Protection des Actifs informationnels

Tous les utilisateurs sont responsables de classifier et de protéger les Actifs informationnels selon leur Degré de sensibilité de l'information et leur Cycle de vie de l'information, afin d'assurer leur Disponibilité, leur Intégrité, leur Confidentialité et leur Traçabilité.

2.1.3 Responsabilité des Utilisateurs et des Intervenants

La protection de l'Information détenue par la SHDM s'appuie sur l'engagement continu de l'ensemble des Utilisateurs. Chacun a l'obligation de protéger l'Information et le matériel mis à sa disposition. Les Intervenants ont des responsabilités spécifiques en matière de sécurité et sont redevables de leurs actions. Ainsi, les rôles et responsabilités des Intervenants sont clairement définis à l'article 2.2.13 de la présente section et dans tous les processus d'affaires de la SHDM.

2.1.4 Sensibilisation et formation

La formation et la sensibilisation à la sécurité informationnelle de manière continue sont essentielles pour assurer la protection des Informations. Ainsi, il importe que les Utilisateurs soient sensibilisés aux menaces et aux conséquences d'une atteinte à la sécurité, qu'ils comprennent leur rôle et leurs obligations ainsi que les procédures de sécurité existantes, qu'ils développent des réflexes et reconnaissent les incidents ou les risques potentiels afin de travailler dans un environnement sécuritaire.

2.1.5 Traitement et signalement des incidents

Toute personne visée par la présente Politique a l'obligation de signaler sans délai au Bureau des technologies de l'information, tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité tel que, le vol, l'intrusion dans un réseau ou système, les dommages délibérés, l'utilisation abusive, la fraude, etc. Le signalement doit se faire soit, via l'adresse supportinfo@shdm.org ou en contactant directement le chef – technologies de l'information.

2.1.6 Contrôle des accès

Toute Information considérée confidentielle ou sensible doit être protégée contre tout accès ou utilisation non autorisés ou illicites. L'accès aux Actifs doit se faire en se basant sur le « besoin de savoir » dans le cadre des fonctions d'un Utilisateur.

2.1.7 Continuité des affaires

La SHDM doit disposer de mesures d'urgence issues de son plan de reprise après sinistre et redondance, consignées par écrit, éprouvées et mises à jour en vue d'assurer la remise (dans un délai raisonnable) des opérations jugées essentielles en cas de sinistre majeur (ex. : incendie, attaque cybernétique, panne électrique prolongée, inondation, malveillance, etc.).

2.1.8 Droit de propriété intellectuelle

Les Utilisateurs doivent se conformer aux exigences légales portant sur l'utilisation de produits à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle, notamment, en ne reproduisant pas et en n'utilisant pas de reproductions illicites de logiciels, de progiciels ou de tout autre forme d'Actifs informationnels, sauf :

- pour des fins de copie de sécurité;
- selon les normes de la licence d'utilisation d'un produit;
- avec le consentement du propriétaire du droit d'auteur;

2.1.9 Droit de regard

La SHDM a un droit de regard et d'intervention, exercé conformément aux lois et règlements, sur l'utilisation de ses Actifs informationnels ainsi que des moyens et des lieux qui permettent d'y accéder.

2.1.10 Intégration au processus d'affaires

La SHDM doit intégrer dans son processus d'affaires, notamment lors de la négociation ou de la conclusion d'ententes et de contrats, des mesures s'adressant aux Intervenants, afin de garantir le respect des exigences de la SHDM en matière de sécurité de l'information.

2.1.11 Mesures d'exception

Aucune dérogation à la présente Politique et à ses documents afférents n'est permise, à moins d'une autorisation écrite du directeur général de la SHDM, laquelle pourra être émise dans les cas d'urgence ou pour corriger toute erreur ou omission matérielle. Toute dérogation à la présente Politique devra faire l'objet d'un compte rendu auprès du conseil d'administration, qui verra à ratifier, ou le cas échéant, à corriger la décision dérogatoire.

2.2 Rôles et responsabilités

2.2.1 Conseil d'administration et comités

- Adopter la Politique ainsi que ses mises à jour;
- Assurer un suivi de la mise en place de la Politique et de son efficience, au moyen d'une reddition de compte. Le registre des incidents à l'égard de la sécurité de l'information est soumis annuellement pour information à ses comités responsables de la Politique qui en font rapport au conseil.

Comités du conseil d'administration

- Les rôles et responsabilités des comités du conseil sont tels que définis au Règlement et mandat des comités du conseil d'administration de la SHDM.

2.2.2 Comité de direction

- S'assurer de l'efficacité et de l'efficience de la Politique ainsi que de l'atteinte de ses objectifs;
- Approuver les mesures de sécurité de l'information ainsi que les objectifs de la Politique.

2.2.3 Chef – technologies de l'information

- Collaborer à l'élaboration et au développement de politiques, de directives, de normes, de procédures et de programmes en matière de sécurité de l'information;
- Veiller à l'application de la Politique;
- Recommander les mesures de sécurité de l'information et en établir les objectifs pour les soumettre au comité de direction.
- Prendre action, de façon diligente, lorsque des décisions sont requises à la suite d'une situation inattendue liée à la sécurité de l'information et qui exige un redressement rapide.
- Veiller à ce que les mesures de sécurité soient mises en place par les Propriétaires d'Actif informationnel.

2.2.4 Avocat – gestion contractuelle et documentaire

- Collaborer à l'élaboration et au développement de politiques, de directives, de normes, de procédures et de programmes en matière de gestion des documents et des archives, visant notamment le traitement, la préservation, la diffusion, la destruction et la conservation de l'Actif informationnel de la SHDM;
- Proposer et veiller à l'application des outils archivistiques, tels que le plan de classification et le calendrier de conservation;
- S'assurer de l'implantation de programmes de formation des Utilisateurs en matière de gestion des documents.

2.2.5 Responsable de la protection des renseignements personnels

- S'assurer de l'implantation de programmes de formation des Utilisateurs en matière de Confidentialité de l'Information et de protection de l'Information sensible.
- Collaborer avec le technicien en informatique dans la gestion des incidents de sécurité ayant un impact sur des renseignements personnels.

2.2.6 Administrateur de systèmes

- Examiner le rendement et l'efficacité du programme de sécurité de l'information de la SHDM et émettre les recommandations appropriées au chef – technologies de l'information.
- Examiner, prioriser et recommander au chef – technologies de l'information les orientations, initiatives ainsi que les projets de sécurité de l'information.
- Procéder à des vérifications de conformité de la Politique.
- Proposer des outils, des mesures de surveillance et des mises à jour des systèmes d'information et de l'équipement.
- Analyser et évaluer les risques de sécurité et signaler tout risque au chef – technologies de l'information.

2.2.7 Technicien en informatique

- Contribuer à l'identification, la localisation et le marquage de l'Actif informationnel.
- Évaluer et réviser périodiquement la sensibilité de l'Actif informationnel en termes de Disponibilité, d'Intégrité, de Confidentialité et de sa valeur.
- Rendre compte de l'état de la sécurité de l'Actif informationnel à l'administrateur de systèmes.
- S'assurer de la réalisation des activités suivantes concernant l'Actif informationnel :
  - la sensibilisation à la sécurité auprès de ses Utilisateurs;
  - la vérification de conformité quant aux mesures mises en place pour le protéger;
  - la gestion d'un incident de sécurité.

2.2.8 Technicien en gestion des documents et archives

- Assister les équipes dans leur mise en application de l'identification, la localisation et le marquage de l'Information;
- Assurer une vigie des structures en place et appliquer le plan de classification et le calendrier de conservation de la SHDM;
- Former les Utilisateurs concernant le plan de classification, le calendrier de conservation et le nommage des documents.

2.2.9 Directeur des affaires juridiques et corporatives

- S'assurer que la SHDM réponde aux exigences légales, réglementaires et contractuelles applicables à cette Politique.

2.2.10 Directeur des ressources humaines, des communications et de l'expérience client

- Informer les Utilisateurs de leurs responsabilités quant au respect de la présente Politique.
- Appliquer les mesures disciplinaires aux Utilisateurs relativement aux infractions à la présente Politique.

2.2.11 Propriétaire d'Actif informationnel

- Assurer la gestion de la sécurité de son Actif informationnel, en veillant à ce que les mesures de sécurité appropriées soient élaborées, mises en place et appliquées.

2.2.12 Utilisateurs

- Prendre connaissance et adhérer à la Politique, ainsi qu'à toutes les directives, lignes directrices, autres politiques, normes ou procédures édictées par la SHDM.
- Utiliser les Actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont accordés.

2.2.13 Intervenants

- Prendre connaissance et adhérer à la Politique, ainsi qu'à toutes les directives, lignes directrices, autres politiques, normes ou procédures édictées par la SHDM.
- Utiliser les Actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui lui sont accordés.

Section 3

3. Non-respect de la Politique

En cas de non-respect de la présente Politique, des directives, des lignes directrices, des normes ou procédures édictées par la SHDM, des mesures administratives, disciplinaires ou légales pourront être appliquées. Ces mesures peuvent inclure la suspension des privilèges d'accès, la réprimande, la suspension, le congédiement ou autre.

Section 4

4. Dispositions finales

Le Bureau des technologies de l'information est responsable de la coordination, de la mise en œuvre et de la mise à jour de la présente Politique.

La présente Politique entre en vigueur dès son adoption par le conseil d'administration de la SHDM.

SHDM

SOCIÉTÉ D'HABITATION ET DE DÉVELOPPEMENT DE MONTRÉAL

800, boulevard De Maisonneuve Est
Bureau 2200
Montréal (Québec) H2L 4L8
Téléphone : 514 380-7436

shdm.org