IDENTIFICATION

Numéro	POL-GI-03
Titre :	Politique globale de sécurité de l'information
Responsable	Direction des technologies de l'information
Historique	Approuvée le 8 septembre 2017 par Louis-Philippe Leblanc Approuvée le 20 septembre 2017 par le directeur général Modifiée le 12 septembre 2019
Statut	En vigueur
Date d'entrée en vigueur	Le 20 septembre 2017

OBJECTIF

- Assurer la sécurité des actifs informationnels, des personnes et des installations de la Ville de Longueuil, notamment en limitant l'accès aux actifs informationnels seulement pour les personnes autorisées, au moment désiré;

- Exprimer la prise de position de la ville visant à faire une saine gestion des risques de sécurité, en fonction des objectifs et contraintes d'affaires de la Ville de Longueuil;

- Permettre à la Ville de Longueuil d'être en mesure d'affronter des défaillances techniques ou humaines, des actes malveillants, ainsi que des sinistres.

ÉNONCÉ

L'information est plus que jamais au cœur de l'optimisation des processus d'affaires. En contrepartie, la sécurité des informations risque d'être compromise si des actions préventives et concrètes ne sont pas systématiquement entreprises lors de l'élaboration des solutions d'affaires électroniques ou lors de l'adoption de pratiques de gestion documentaire et de leur évolution tout au long de leur cycle de vie. Ces risques d'affaires à l'égard de la sécurité des informations peuvent être de nature juridique, stratégique ou financière, entacher la réputation de la ville et ébranler la confiance des citoyens envers elle.

La Ville de Longueuil reconnait l'importance de la sécurité de l'information et la contribution que ce domaine apporte à la réalisation de sa mission en protégeant sa renommée et la confiance des citoyens et d'autres intervenants à l'égard de ses services.

Il est donc approprié de mettre en place un programme de gestion de la sécurité de l'information qui est conforme aux attentes de la ville. Ce programme doit aussi tenir compte des dimensions organisationnelles, humaines, juridiques, financières et technologiques particulières à la ville.

La présente politique établit donc les principes que la ville entend appliquer pour assurer la sécurité de l'information qu'elle traite, gère et manipule dans le cadre de ses opérations. La ville s'engage à supporter tous ces principes ainsi que les mécanismes qui en découlent.

CHAMP D'APPLICATION

Cette politique s'applique à tous les employés de la Ville de Longueuil, aux dirigeants et élus ainsi qu'aux firmes externes ou tiers qui utilisent l'information ou accèdent aux actifs informationnels de la ville en vertu d'une autorisation. Finalement, elle s'applique à tous les actifs informationnels possédés ou utilisés par la ville.

DÉFINITION

Programme de gestion de la sécurité de l'information
Ensemble des éléments (politiques, Directives, procédures, comités, projets, taches opérationnelles, etc.) permettant l'atteinte des objectifs fixés par la Ville en matière de sécurité de l'information.

Information
Information sous toutes formes (écrite, alphanumérique, numérique, sonore, graphique, imagée, photographique, symbolique, dessinée, etc.), sur tout support médiatique ou canal de communication.

Document
Tout type de fichier contenant des informations présentées sous une forme organisée (texte, fiche, liste, tableau, graphique, image, etc.) et consignée, quel qu'en soit le support médiatique.

Système, technologie de l'information ou de communication
Est considéré comme tel notamment : une base de données, une application, un programme, un logiciel, un équipement informatique ou de télécommunication, un espace virtuel, un ordinateur, une imprimante, un télécopieur, un téléphone, un téléphone intelligent, une tablette électronique, un émetteur de radio, un organiseur personnel, un numériseur, etc.

Actif informationnel
Toute information, document, système et technologie de l'information ou de communication.

Criticité
Détermination du degré d'importance de la disponibilité d'un actif informationnel en fonction d'une échelle de gradation commune.

Classification de l'information
Identification de la valeur de l'information pour l'organisation dans le but d'assurer un niveau de protection approprié (public, interne ou confidentiel) selon les principes d'intégrité, de confidentialité et de disponibilité. Cet exercice est conduit en partenariat avec le service de la gestion des documents et des archives (SGDA).

Direction propriétaire
Direction qui a été désignée propriétaire d'un actif par la direction des technologies de l'information (DTI). Il s'agit habituellement de la direction qui produit l'information ou le document ou encore qui est responsable des règles d'affaires entourant l'utilisation d'un système.

Responsable d'un actif informationnel
Cadre qui a été désignée par la direction propriétaire d'un actif pour prendre en charge la responsabilité de la sécurité de celui-ci, notamment en faisant la classification et en donnant les autorisations d'accès. Le registre des responsables d'actifs est maintenu dans le système de gestion de configuration, par leur assignation aux « items de configuration » (CI).

Objectifs de la sécurité de l'information

- **Disponibilité :** Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.
- **Intégrité :** Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation.
- **Confidentialité :** Propriété d'une information de n'être accessible ou divulguée qu'aux personnes ou entités désignées et autorisées.

Plan de continuité des opérations
Est à la fois le nom d'un concept, d'une procédure et du document qui la décrit. Il permet à une organisation de fonctionner même en situation de désastre, en mode dégradé. Son objectif est de minimiser les impacts d'une crise ou d'une catastrophe naturelle, technologique ou sociale sur l'activité (et donc la pérennité) d'une organisation.

Plan de reprise des activités
Plan qui décrit comment reprendre les opérations des services essentiels suite à une interruption de ceux-ci ou encore après une catastrophe.

RÉFÉRENCE

Les lois et directives doivent être considérées comme guides et références aux fins de définition des contrôles et mesures adoptées et mises à jour par la ville. Parmi les lois et directives qui ont une incidence, on retrouve notamment:

- Les lois d'application générale telles que la Loi sur l'administration publique, le Code civil, le Code criminel, la Loi concernant le cadre juridique des technologies de l'information, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;
- Les lois d'application spécifique qui encadrent la mission de la ville;
- Les directives et politiques émises par la ville.

Une liste non exhaustive des lois, règlements et normes en vigueur est présentée en Annexe 2.

PÉRIODE D'APPLICATION

La présente politique entre en vigueur dès son approbation.

CONTENU

1 PRINCIPES DIRECTEURS ET ORIENTATIONS

La présente politique de la Ville de Longueuil énonce que :

1.1 Gestion de la sécurité

- Un comité de sécurité de l'information est créé et est formé de dirigeants de l'organisation (voir la composition du comité en Annexe 1);
- Le responsable de ce comité est le directeur des technologies de l'information;
- Le comité de sécurité de l'information a la responsabilité d'accompagner les responsables d'actifs dans la réalisation des analyses de risques nécessaires à la saine gestion de la sécurité ainsi que d'approuver l'acceptation ou le traitement des risques résiduels.

1.2 Gestion du risque

- L'appréciation du risque prévoit l'évaluation et la comparaison systématique de l'ampleur de ce dernier par rapport au niveau acceptable afin d'en déterminer l'importance;
- Une appréciation du risque est réalisée au minimum annuellement afin de prendre en compte les modifications des exigences de sécurité et de l'exposition au risque, par exemple : actifs informationnels en format électronique ainsi qu'en format papier, menaces, vulnérabilités, impacts, évaluation du risque et moments auxquels des modifications importantes sont effectuées;
- Les résultats de cette évaluation doivent guider et déterminer les actions pertinentes et appropriées pour gérer les risques de sécurité de l'information et pour mettre en place les contrôles identifiés pour se protéger contre ces risques jugés non acceptables, et pour accepter les risques résiduels.

1.3 Gestion des actifs informationnels

- Pour chacun des actifs informationnels de la ville, un responsable à la direction propriétaire de l'actif et la DTI ont une responsabilité partagée relativement à la sécurité de l'information. Par exemple :
    - La direction des Finances est responsable de l'actif informationnel des financiers d'oracle. Les finances sont responsables d'accorder des accès à cet actif selon un processus formel et documenté. La (DTI) est responsable de l'intégrité des données lors d'échange entre différents systèmes d'informations ainsi que de la disponibilité de l'infrastructure technologique supportant cet actif.
- La criticité de chaque actif informationnel est déterminée par son responsable en regard de son importance aux affaires de la ville et de la classification des informations qui s'y rattachent.
- La sécurité des actifs informationnels sera également assurée en fonction du respect du cadre législatif et administratif applicable. Ceci inclut la conformité aux exigences légales en matière de propriété intellectuelle et de droit d'auteur.

1.4 Gestion des opérations et des télécommunications

- Les technologies de l'information et des communications sont gérées et opérées via des processus visant à minimiser les incidents de sécurité et maximiser leur disponibilité.

1.5 Sécurité liée aux ressources humaines

- Les employés, contractuels, stagiaires, apprentis et toute autre personne travaillant pour la ville et devant accéder ou utiliser les actifs informationnels de la ville, peuvent être soumis à des contrôles de sécurité, en conformité avec les pratiques prévues par la direction des ressources humaines.

1.6 Gestion des identités et des accès

- L'accès à un actif informationnel doit être donné à un utilisateur sur la base des tâches qu'il doit accomplir dans le cadre des fonctions qui lui sont attribuées;
- Toutes les attributions de droits d'accès sont faites en conformité avec la ***Directive sur la gestion des identités et des accès logiques et physiques***.

1.7 Gestion des accès physiques

Des mesures de contrôles sont mises en place et maintenues afin de protéger les installations, les employés et les actifs informationnels essentiels contre les accès non autorisés en conformité avec la ***Directive sur la gestion des identités et des accès logiques et physiques***.

1.8 Gestion de la continuité des affaires

- Les moyens nécessaires sont déployés pour assurer la disponibilité des actifs informationnels selon leur criticité établie en fonction de la classification des informations qui s'y rattachent :
    - Chaque direction est responsable de mettre en place un plan de continuité des opérations de son secteur d'affaires;
    - Le comité de sécurité de l'information s'assure que les directions mettent en place les plans de continuité nécessaires.
    - Les plans de la continuité des affaires et les plans de relève doivent être revus et testés périodiquement.
- À l'intérieur de leurs plans de continuité des opérations, chaque direction définit les modes de livraison des différents services en l'absence de la disponibilité de certains actifs informationnels :
    - La DTI est responsable de la disponibilité de l'aspect infrastructure technologique des actifs informationnels;
    - La DTI propose aux directions une démarche de continuité type, basée sur les bonnes pratiques du marché.

1.9 Gestion des tierces parties

- Les actifs informationnels sont la propriété exclusive de la Ville de Longueuil en tenant compte des ententes contractuelles, accords de licences, prêts, utilisations et cessions avec de tierces parties. Des règles sont conventionnées avec les tiers, afin d'assurer la préservation des attributs de sécurité des actifs informationnels dont la ville est propriétaire ou responsable.

1.10 Acquisition, développement et maintenance des systèmes d'information

Les exigences de sécurité doivent être identifiées, définies et révisées tout au long du cycle de vie d'un actif informationnel (acquisition, développement et mise à niveau). Elles doivent être identifiées en même temps que les exigences générales d'un projet et doivent être justifiées, reconnues et documentées dans le cadre de la gestion générale d'un système d'information.

1.11 Chiffrement et gestion des clés

- Les opérations de chiffrement doivent utiliser un processus standard et identifiable réputé comme sécuritaire par l'industrie.
- Les clés de chiffrement doivent être protégées et être gérées de façon à être récupérées, remplacée ou révoquée au besoin.

1.12 Sécurité physique et environnementale

- Des contrôles visant à protéger l'infrastructure physique et les systèmes contre les risques environnementaux doivent être mise en place.

2 GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

2.1 La direction générale

- Approuve la présente politique et toute modification.

2.2 Toutes les directions

- Chaque direction est responsable de faire appliquer les principes directeurs contenus dans la présente politique et tous les encadrements administratifs en découlant, ainsi que d'en rendre compte dans sa ligne hiérarchique.
  - Participer aux analyses de risques.
  - Établir la criticité des actifs.
  - Exécuter les contrôles identifiés pour protéger les actifs informationnels.
  - Mettre en place un plan de continuité des affaires.

2.3 La direction des technologies de l'information

- S'assure d'une saine gestion des risques par l'adoption d'une stratégie de gestion de risques qui répond aux impératifs d'affaires de la ville et tient compte des dimensions organisationnelles, humaines, juridiques, financières et technologiques;
- Évalue la performance de la gestion des risques, fait rapport au comité de sécurité de l'information et émet les recommandations appropriées;
- Évalue les besoins en encadrements et propose les changements appropriés à la direction générale et maintiens un registre de ses activités de sécurité;
- Gère le programme de sensibilisation en sécurité de l'information;
- Tiens la direction générale informée des incidents importants en matière de sécurité et des actions entreprises pour y remédier;
- Consulte régulièrement les autres directions pour lesquelles la sécurité de l'information est pertinente.

2.4 Le comité de sécurité de l'information

- Décide des orientations en sécurité de l'information à l'égard des recommandations provenant notamment, mais sans s'y limiter de la Direction générale, du bureau de la Vérificatrice générale et des Ressources informationnelles;
- Réévalue au minimum annuellement la présente politique et s'assure qu'elle répond aux orientations, objectifs, exigences d'affaires et cadre législatif de la ville.

2.5 La direction des ressources matérielles

- S'assure que tout contrat approuvé intègre les clauses pertinentes de sécurité de l'information.

2.6 La direction des ressources humaines

- S'assure que les employés sont sensibilisés à la sécurité de l'information lors de leur embauche;
- S'assure que les clauses de la présente politique sont tenues en compte dans les ententes entre la ville et ses employés;
- Effectue les contrôles de sécurité prévus, tel la vérification d'antécédents, lors de l'embauche de nouveaux employés, ainsi qu'à tout autre moment préalablement déterminé avec les directions concernées.

2.7 Le responsable d'un actif informationnel

- Est désigné par la direction propriétaire de l'actif informationnel;
- Applique la sécurité de cet actif en conformité avec la présente politique et ses encadrements administratifs;
- Gère les risques de cet actif informationnel : de l'identification des vulnérabilités, en passant par l'identification des menaces, l'analyse de potentialité des risques et des impacts sur les affaires, la planification, le choix ainsi que la mise en œuvre des mesures d'atténuation de risques, jusqu'à l'évaluation des risques résiduels;

- Gère les incidents de sécurité : divulgue tout incident de sécurité au directeur des
- technologies de l'information et met en œuvre les mesures correctives pour en prévenir la répétition;
- Informe et sensibilise les utilisateurs à l'égard de la sécurité des actifs informationnels sous sa responsabilité dans le but de réduire les risques.

2.8 Tous les utilisateurs des actifs informationnels

- Respectent les principes directeurs contenus dans la présente politique ainsi que tous les encadrements administratifs en découlant.

3 SANCTIONS

La ville peut imposer des sanctions aux contrevenants, incluant prendre contre ceux-ci tout recours civil approprié, s'il est démontré qu'une inconduite ou une négligence a engendré un incident de sécurité.

ANNEXE 1 – COMITÉ DE SÉCURITÉ DE L'INFORMATION – ORGANIGRAMME

Comité de sécurité de l'information

Pilote : Ressources informationnelles

Membres :

1 Direction générale
2 Ressources humaines (Relations de travail et liens avec employés)
3 Travaux publics (Accès physiques
4 Contentieux (Lois applicables)
5 Greffe – Service de la gestion des documents et archives (Conservation de l'information)
6 SPAL (Menaces et vérifications)
7 Autres directions selon sujets ponctuels

Équipe de sécurité opérationnelle (DTI)

ANNEXE 2 – CADRE LÉGAL ET ADMINISTRATIF (EN RÉVISION)

1) LA CHARTE CANADIENNE DES DROITS ET LIBERTÉS (1982), L.R.C. (1985), App. II, no 44

2) LOI SUR LA PREUVE L.R.C. (1985) ch. C-5

http://lois.justice.gc.ca/fra/lois/c-5/

3) LE CODE CRIMINEL, L.R.C. 1985, c. C-46

http://lois.justice.gc.ca/fra/lois/C-46/

4) LA LOI SUR LE DROIT D'AUTEUR, L.R.C. (1985),c, C-42

http://lois.justice.gc.ca/fra/lois/C-42/

5) LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES, L.C. (2000), ch. C-5

http://lois.justice.gc.ca/fra/lois/p-8.6/

6) CHARTE DES DROITS ET LIBERTÉS DE LA PERSONNE, L.R.Q., chapitre C-12

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_12/C12.HTM

7) CODE CIVIL DU QUÉBEC, C.c.Q. (1991), chapitre C-64

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/CCQ/CCQ.html

8) LOI CONCERNANT LE CADRE JURIDIQUE DES TECHNOLOGIES DE L'INFORMATION L.R.Q., chapitre C-1.1

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1.html

9) LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, L.R.Q., chapitre A-2.1;

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=%2F%2FA_2_1%2FA2_1.htm

10) LOI SUR LES ARCHIVES, L.R.Q., chapitre A-21.1

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=//A_21_1/A21_1.html

11) LOI SUR LES CITÉS ET VILLES L.R.Q., chapitre C-19

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_19/C19.html

12) LOI SUR LES COMPÉTENCES MUNICIPALES L.R.Q., chapitre C-47.1

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_47_1/C47_1.html

13) LOI SUR L'EXERCICE DE CERTAINES COMPÉTENCES MUNICIPALES DANS CERTAINES AGGLOMÉRATIONS L.R.Q., chapitre E-20.001

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=%2F%2FE_20_001%2FE20_001.htm

14) CHARTE DE LA VILLE DE LONGUEUIL L.R.Q., chapitre C-11.3

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_11_3/C11_3.html

15) *LOI SUR LA GOUVERNANCE ET LA GESTION DES RESSOURCES INFORMATIONNELLES DES ORGANISMES PUBLICS ET DES ENTREPRISES DU GOUVERNEMENT*

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/G_1_03/G1_03.html

16) *Décret 7-2014 concernant la* DIRECTIVE SUR LA SÉCURITÉ DE L'INFORMATION GOUVERNEMENTALE, (2014) 146 G.O II 427

http://www.tresor.gouv.qc.ca/ressources-informationnelles/securite-de-linformation/directive-sur-la-securite-de-linformation-gouvernementale/

17) NORME ISO/IEC 27001:2013 – Management de la sécurité de l'information

http://www.iso.org/iso/fr/home/standards/management-standards/iso27001.htm

18) NORME PCI-DSS (Payment Card Industry DATA Security Standard)

https://fr.pcisecuritystandards.org/minisite/en/

19) NORME FIPS 140-3 (Security requirements for Cryptographic Modules)

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf