Politique de sécurité de l'information

Adopté : Le 1er août 2011

Table des matières

1. La sécurité de l'information

La sécurité de l'information revêt de plus en plus d'importance dans notre société. Les échanges accélérés d'information à l'aide de moyens technologiques hautement sophistiqués en facilitent la diffusion et l'accès. La probabilité de manipulation à des fins illégitimes en est augmentée et l'impact est plus grande. On n'a qu'à penser notamment aux vols d'identité, aux fraudes financières, à la destruction non autorisée de documents ou à l'infiltration illégale dans les réseaux de télécommunications.

L'information est présente sous toutes ses formes et à tous les niveaux au sein de l'organisation. Elle est utilisée entre autres pour les opérations administratives, les échanges avec les citoyens et les partenaires, pour assurer les services municipaux et la sécurité des citoyens. Une mauvaise utilisation de l'information peut ternir l'image et la réputation de la Ville, mettre en danger la sécurité des citoyens, engager sa responsabilité, rendre vulnérables les équipements et infrastructures municipales névralgiques, nuire aux opérations administratives ou entraîner des pertes financières pour la municipalité.

La Ville reconnaît que l'information est essentielle à ses opérations courantes et, de ce fait, qu'elle doit faire l'objet d'une évaluation, d'une utilisation et d'une protection appropriées. Elle reconnaît détenir en outre des renseignements personnels ainsi que des informations qui ont une valeur légale, administrative, économique ou patrimoniale. La Ville doit veiller au respect des lois, règlements, directives et normes qui lui sont applicables en matière de sécurité de l'information. La volonté de la Ville est de mettre en place des mesures pour assurer une protection adéquate de ses actifs informationnels. La Ville adopte par conséquent la présente politique de sécurité de l'information qui oriente et détermine leur utilisation appropriée et sécuritaire.

2. Définitions

Actif informationnel : ensemble des documents et des informations, numériques ou non, des banques de données, des systèmes d'information, des technologies de l'information, acquis ou constitué par la Ville et sous sa responsabilité.

Bases de données : regroupement d'un ensemble d'informations numériques classées selon un certain ordre.

Collecticiel : logiciel qui permet à des utilisateurs reliés par un réseau de travailler en collaboration sur un même projet.

Confidentialité : propriété d'une information ou de renseignements personnels qui ne doivent pas être divulgués à des personnes ou à des entités non autorisées.

Courriel : service de correspondance sous forme d'échange de messages électroniques par un réseau informatique.

Cycle de vie : ensemble des étapes que franchit l'information et qui vont de sa création ou sa collecte, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction en conformité avec le calendrier de conservation de la Ville.

Disponibilité : propriété qu'ont les données, l'information et les systèmes d'information d'être accessibles et utilisables à la demande par une entité autorisée.

Document : ensemble d'informations entreposées sur un support, sous une forme permanente et lisible par une personne ou par un moyen mécanique ou électronique.

Gestion de la sécurité de l'information : gérer la sécurité de l'information dans une organisation, c'est organiser l'information, implanter une politique et des procédures d'ensemble qui assurent la sécurité des données, assurer une bonne gouvernance, désigner un responsable, allouer un budget, réaliser des actions de sensibilisation et de formation, gérer les incidents et prévoir des processus réguliers de révision et d'évaluation.

Information : renseignements consignés sur un support quelconque dans un but de transmission des connaissances.

Information numérique : information dont l'utilisation n'est possible qu'au moyen des technologies de l'information.

Intégrité : propriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle et conservent un format permettant leur utilisation.

Matrice de catégorisation : document identifiant différents systèmes d'information, les cotes attribuées en termes de disponibilité, d'intégrité et de confidentialité de l'information. Cette matrice permet de déterminer les mesures de sécurité à mettre en place, touchant les volets juridiques, organisationnels, humains et technologiques.

Processus d'affaires : ensemble des actions qui doivent être accomplies successivement pour parvenir au résultat recherché.

Propriétaire de l'actif informationnel : gestionnaire à qui est assignée la responsabilité de la sécurité de l'information, d'une technologie de l'information ou d'un processus d'affaires. Ce terme ne signifie pas que la personne jouit de droits de propriété sur l'actif informationnel. L'utilisation de ce terme est conforme aux Normes de la série ISO 27000.

Registre d'autorité : répertoire, recueil ou fichier dans lesquels sont inscrites les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité, ainsi que les responsabilités qui y sont rattachées. Par exemple, on y retrouve l'identification des systèmes informatiques et le principal propriétaire pour chacun d'eux, soit le répondant administratif du système.

Registre des incidents : registre permettant de consigner différents incidents de sécurité, qu'ils soient réels ou suspectés, ou qu'il s'agisse d'une tentative d'atteinte à la sécurité susceptible d'affecter la disponibilité, l'intégrité et la confidentialité d'un actif informationnel, de les documenter, d'identifier les mesures mises en place pour corriger la situation et éviter qu'elle ne se reproduise.

Risque : probabilité que survienne un événement nuisible et éventualité qu'existe une menace plus ou moins prévisible pouvant influer sur la réalisation des objectifs de la Ville.

Sécurité de l'information : la sécurité de l'information (SI) est l'état de protection des actifs informationnels face aux risques identifiés. Cet état, aussi appelé « niveau de confiance », résulte de l'ensemble des mesures de sécurité prises par la Ville pour préserver la confidentialité, l'intégrité et la disponibilité de l'information qu'elle détient, quel que soit son support (papier, électronique, etc.).

Système de gestion de la sécurité de l'information (SGSI) : partie du système de gestion global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information. Le SGSI fait référence au cadre de gestion.

Système d'information : ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y compris notamment les technologies de l'information et les procédés aménagés pour accomplir ces fonctions.

Technologie de l'information : toute combinaison d'équipements informatiques (ex. : ordinateur, imprimante, numériseur, clé USB), de logiciels, de collecticiels, d'Internet, d'intranet, de programmes, d'applications et de systèmes permettant de créer, d'emmagasiner, de traiter, de manipuler, de communiquer, de protéger et d'éliminer de l'information numérique.

Ville : la Ville de Laval.

3. Objectif général

L'objectif de la politique de sécurité de l'information est de mettre en place des règles concernant l'utilisation et la protection de l'information, et ce, tout au long de son cycle de vie. Ces règles découlent notamment des lois, des règlements, des normes, des directives, des procédures administratives et des contrats. Elles visent la protection de l'information par l'élaboration de mesures cherchant à en assurer la disponibilité, l'intégrité et la confidentialité durant tout son cycle de vie. Les bases de la politique de sécurité de l'information reposent sur l'établissement d'un cadre de gestion de la sécurité de l'information définissant les mesures à implanter pour la réduction du risque et un processus d'amélioration continu. Le cadre de gestion vise à attribuer formellement l'ensemble des responsabilités corporatives en matière de protection de l'information. Il définit une structure de gouvernance qui permet une gestion continuelle des risques en sécurité, de même que l'étendue du domaine couvert par la sécurité de l'information. Par la suite, des directives, procédures, standards suivront pour la mise en opération de la politique de sécurité de l'information en fonction du niveau hiérarchique.

L'objectif de cet encadrement est de limiter l'impact des dysfonctionnements en s'assurant notamment :

- d'orienter et de positionner la Ville en matière de sécurité de l'information;
- d'assurer un service continu, efficace et efficient à l'information pour les citoyens, les employés et les autres utilisateurs autorisés;
- de préciser la portée de la sécurité de l'information à travers les activités et la structure de la Ville;
- de respecter la conformité aux lois, à la réglementation, aux normes, aux directives et aux procédures administratives applicables;
- de limiter les pertes financières;
- de collaborer avec les partenaires en respectant les ententes contractuelles;
- de s'assurer du bon déroulement des prises de décisions et du processus démocratique;
- de protéger l'image et la réputation de la Ville comme organisme public responsable.

4. Domaine d'application

L'information se présente sur des supports variés. Elle peut être disponible sur tout dispositif apte à la stocker : support papier, électronique, audiovisuel, sonore ou autre. La présente politique s'applique à tout actif informationnel, et ce, quel que soit son support.

Les actifs informationnels appartiennent à la Ville ou elle peut en être une utilisatrice autorisée en vertu notamment d'ententes contractuelles, d'accords de licences, de prêts ou de cessions. Ils peuvent être conservés ou utilisés par un tiers à l'intérieur ou à l'extérieur des locaux de la Ville. Ce tiers doit se soumettre à la présente politique et, le cas échéant, aux règles conventionnées afin d'assurer la disponibilité, l'intégrité et la confidentialité des actifs informationnels.

Les utilisateurs visés sont toute personne physique ou morale ayant accès de près ou de loin à l'information sous la gouverne de la Ville. Il s'agit des employés sans égard à leur catégorie d'emploi ou de statut (permanent, occasionnel, contractuel, stagiaire, gestionnaire, etc.), des citoyens, des élus, des fournisseurs, des partenaires, des utilisateurs de services provenant de l'extérieur et des autorités. Les utilisateurs visés doivent se soumettre à la présente politique.

5. Principes directeurs et orientations

Les énoncés suivants constituent les orientations que se donne la Ville en matière de gestion de sécurité de l'information. Pour ce faire, la Ville doit assurer la sécurité de ses informations conformément aux principes directeurs ci-dessous.

Les principes directeurs régissant la sécurité de l'information sont la disponibilité, l'intégrité et la confidentialité. Ils s'assurent respectivement de l'accès à l'information, de la fiabilité de l'information et de la consultation autorisée à l'information.

Compte tenu de la complexité et des coûts associés à l'élaboration de ces principes directeurs, la Ville met en place un cadre de gestion de la sécurité de l'information basé sur l'identification et l'évaluation périodique des risques qui menacent la disponibilité, l'intégrité et la confidentialité de l'information afin d'en réduire la portée et de les maintenir à un niveau acceptable pour l'organisation. Le cadre de gestion s'appuie également sur l'amélioration continue.

Les mesures de protection sont appliquées selon les objectifs de la politique de sécurité, les lois et règles, les exigences opérationnelles, les coûts et les dommages potentiels.

Les principes directeurs et orientations visent notamment à :

- classifier les actifs informationnels selon leur degré de sensibilité et selon les exigences qui y sont liées pour assurer leur sécurité;
- protéger les actifs informationnels;
- conserver l'intégrité des actifs informationnels;
- assurer la confidentialité de l'information;
- sensibiliser de manière continue les employés à la sécurité des actifs informationnels et aux conséquences d'une atteinte à la sécurité;
- assurer un accès continu aux actifs informationnels aux citoyens, aux employés et aux autres utilisateurs autorisés;
- conserver l'information et à s'assurer de sa destruction sécuritaire;
- s'assurer de la conformité aux lois, règlements, procédures administratives ou ententes contractuelles;
- gérer les budgets de sécurité d'une manière efficiente en tenant compte des risques;
- maintenir et protéger l'image et la réputation de la Ville comme organisme public responsable;

- fournir un support aux autorités lors de l'utilisation malveillante des actifs informationnels de la Ville;
- mettre en œuvre des règles permettant l'utilisation adéquate des actifs informationnels;
- assurer la continuité des activités nécessaires à la mission de la Ville lors d'un sinistre ou d'une défaillance majeure affectant les actifs informationnels jugés essentiels.

Les normes de la série ISO 27000 (ISO 27001 et ISO 27002) de l'Organisation internationale de normalisation font partie du cadre de gestion pour la mise en place de la politique de sécurité de l'information de la Ville. Ces normes internationales édictent les meilleures pratiques en termes de gestion de la sécurité de l'information.

6. Cadre juridique, normatif et contractuel

Il est primordial d'éviter toute violation des obligations légales, réglementaires, normatives ou contractuelles et d'en respecter les exigences de sécurité de l'information et de la protection des renseignements personnels, de même que la protection des droits de propriété intellectuelle.

Les lois, règlements, directives, règles, politiques et normes servant de cadre de référence à la présente politique sont notamment :

- la *Charte canadienne des droits et libertés* (Annexe B de la Loi de 1982 sur le Canada, 1982, chapitre 11 (R.-U.);
- *la Charte des droits et libertés de la personne* (L.R.Q., chapitre C-12);
- le *Code civil du Québec* (L.Q., 1991, chapitre 64);
- le *Code criminel du Canada* (L.R.C., 1985, chapitre C-46);
- le *Code des professions* (L.R.Q., chapitre C-26) et les différentes lois régissant les professions pour certaines applications;
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q. chapitre A-2.1);
- la *Loi sur les archives* (L.R.Q., chapitre A-21.1);
- la *Loi sur les brevets* (L.R.C. 1985, chapitre P-4);
- la *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., chapitre C-1.1);
- la *Loi sur les cités et villes* (L.R.Q., chapitre C-19);
- la *Loi sur le droit d'auteur* (L.R.C. chapitre C-42);
- la *Loi sur la fiscalité municipale* (L.R.Q., chapitre F-2.1);
- la *Loi sur les marques de commerce* (L.R.C., 1985, chapitre T-13);
- la *Loi sur la police* (L.R.Q., chapitre P-13.1);
- la *Loi sur la qualité de l'environnement* (L.R.Q., chapitre Q-2);
- la *Loi sur la santé et la sécurité du travail* (L.R.Q., chapitre S-2.1);
- la *Loi sur la sécurité civile* (L.R.Q., chapitre S-2.3);
- la *Loi sur la sécurité incendie* (L.R.Q., chapitre S-3.4);
- les Normes de la série ISO 27000 (ISO 27001 et ISO 27002) de l'Organisation internationale de normalisation;
- la Politique d'approvisionnement de la Ville (Résolution CE-2010/8589);
- la Politique de gestion contractuelle de la Ville (Résolution 2010/844);
- la Politique de gestion intégrée des documents de la Ville (Résolution 2008/788);
- les dispositions de tout code d'éthique adopté par la Ville applicable aux élus et aux employés municipaux.

Enfin, certaines ententes contractuelles peuvent imposer à la Ville, des politiques et procédures spécifiques. Ces ententes concernent notamment l'utilisation des données des autres corps de police, les licences de logiciels, les ententes avec les fournisseurs ou partenaires et les conventions collectives.

Dans le cas d'ambigüité entre ces ententes et la présente politique, la plus restrictive prédomine.

7. Conséquences de la violation

Les conséquences de la violation des règles de la politique de sécurité de l'information diffèrent selon le type d'utilisateur des actifs informationnels, c'est-à-dire :

- tout citoyen ou utilisateur peut notamment se voir retirer son droit d'accès sur le champ et faire l'objet de poursuites judiciaires;
- tout membre du personnel, quel que soit la catégorie d'emploi ou de statut, peut être passible de sanctions administratives, disciplinaires ou légales modulées en fonction du principe de la gradation des sanctions et en fonction de la gravité, du contexte et des conséquences de son geste, et ce, conformément aux dispositions des ententes ou des conventions collectives applicables. Une contravention à la présente politique par un membre du personnel peut notamment mener à un retrait de son droit d'accès sur le champ, à une réprimande, à une suspension sans salaire ou à un congédiement, de même qu'à des poursuites judiciaires;
- tout partenaire, mandataire, consultant ou fournisseur peut notamment se voir retirer son droit d'accès sur le champ, résilier unilatéralement son contrat et faire l'objet de poursuites judiciaires.

8. Gouvernance

La gouvernance de la sécurité de l'information fait partie intégrante de la gouvernance d'entreprise. Elle consiste dans le leadership et l'organisation des structures et processus qui assurent que la sécurité de l'information soutient et prolonge la stratégie et les objectifs de l'organisation.

Des comités aux niveaux stratégiques, tactiques et opérationnels ont été constitués pour assurer la gouvernance et l'amélioration continue de la sécurité de l'information. D'autres comités pourront s'ajouter au fur et à mesure que la politique sera mise en opération.

Aussi, les rôles et responsabilités de l'organisation interne de la Ville sont définis dans le cadre de la présente politique.

8.1 Structure de gouvernance

Le Conseil municipal

- Approuve les orientations générales soumises par le Comité exécutif en matière de sécurité de l'information;
- Suite aux recommandations du Comité exécutif, adopte tout changement à la politique de sécurité de l'information.

Le Comité exécutif

- Recommande au Conseil municipal d'approuver les orientations générales en matière de sécurité de l'information;
- Recommande au Conseil municipal d'adopter tout changement à la politique de sécurité de l'information.

La Direction générale

- Soutient activement la politique de sécurité de l'information au sein de l'organisation au moyen de directives claires, d'un engagement franc, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information;

- Fournit les ressources nécessaires au bon fonctionnement du système de gestion de sécurité de l'information (SGSI).

Le Comité de sécurité de l'information (CE-2009/4063)

Sous l'autorité du Comité exécutif et de la Direction générale, notamment il :

- Soutient la Direction générale dans l'exercice de ses responsabilités et l'exécution de ses obligations en matière de sécurité de l'information;
- Intervient au niveau stratégique;
- Aligne la politique de sécurité de l'information avec les objectifs et la stratégie de l'organisation;
- Fixe les objectifs et la stratégie du système de gestion de la sécurité de l'information (SGSI);
- Valide la politique de sécurité de l'information;
- Approuve les critères d'acceptation du risque et les risques résiduels;
- Revoit tous les aspects relatifs à l'accès aux documents, à la protection des renseignements personnels et à la sécurité de l'information;
- Assure une approche intégrée en sécurité en considérant tous les aspects de la sécurité de l'information en ce qui concerne autant l'information elle-même (disponibilité, intégrité, confidentialité), l'individu qui y a accès (habilitation de niveau approprié), l'accès physique aux lieux (système d'alarme, serrure, environnement physique), que les aspects administratifs et légaux assurant sa protection;
- Recommande les orientations, établit les priorités et tient lieu de forum de coordination et de concertation relativement à l'accès à l'information, à la protection des renseignements personnels et à la sécurité de l'information;
- Établit les mesures particulières à respecter en matière de protection des renseignements personnels relatives aux sondages recueillant ou utilisant des renseignements personnels et à l'utilisation d'une technologie de vidéosurveillance;

- Détermine, parmi les projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de service qui recueille, utilise, conserve, communique ou détruit des renseignements personnels, ceux qui doivent être encadrés par des mesures particulières de protection des renseignements personnels et de sécurité de l'information;

- Présente au Comité exécutif et à la Direction générale ses recommandations relatives aux orientations générales de la Ville en matière de sécurité de l'information et à tout changement à la politique de sécurité de l'information;

- Autorise la mise en œuvre et l'exploitation du système de gestion de la sécurité de l'information (SGSI);

- Crée, au besoin, différents comités et suit l'avancement de leurs travaux.

Le responsable de la sécurité de l'information

Sous l'autorité du directeur du Service des systèmes et des technologies, notamment il :

- Soutient le Comité de sécurité de l'information dans la détermination des orientations stratégiques et des priorités d'intervention en matière de sécurité de l'information et en coordonne l'ensemble des activités;

- Voit à la sensibilisation du personnel, des gestionnaires et de toute personne utilisant ou accédant aux informations détenues par la Ville relativement aux obligations et aux pratiques en matière d'accès à l'information, de la protection des renseignements personnels et de la sécurité de l'information;

- S'assure de l'élaboration, de la mise à jour et de l'approbation par le Comité de sécurité de l'information des mesures de sécurité en vue d'assurer la protection des renseignements personnels (collectés, utilisés, conservés, communiqués ou détruits);

- Fait approuver par le Comité de sécurité de l'information, les documents et activités du plan d'action stratégique en sécurité de l'information et ceux ayant une incidence tactique ou opérationnelle;

- S'assure de l'identification et de la gestion des risques d'atteinte à la sécurité de l'information et identifie les risques résiduels qui doivent être assumés par le Comité de sécurité de l'information et l'en informe;
- Assure la cohérence et la pertinence des interventions en matière de sécurité de l'information;
- Coordonne et voit à la réalisation de la catégorisation de l'information et des processus d'affaires ainsi que des analyses de risques en matière de sécurité de l'information;
- Assure le suivi de la politique de sécurité de l'information;
- Présente au Comité de sécurité de l'information, pour approbation, un plan global de sécurité visant à renforcer l'état de la sécurité de l'information;
- Élabore, met en place et maintient à jour le plan de relève des actifs informationnels et des processus d'affaires critiques désignés par les propriétaires des actifs informationnels;
- Crée et met à jour le registre d'autorité, le registre des incidents ainsi que la matrice de catégorisation.

Le Comité de pilotage de la politique de sécurité de l'information

Sous l'autorité du responsable de la sécurité de l'information, notamment il :

- Intervient au niveau tactique et opérationnel de l'organisation;
- Gère l'implantation de la politique de sécurité de l'information;
- Planifie la mise en œuvre du système de la gestion de la sécurité de l'information (SGSI);
- Définit la politique du système de la gestion de la sécurité de l'information (SGSI) en adéquation avec les objectifs définis par le Comité de sécurité de l'information;
- Propose les rôles et responsabilités;
- Définit la méthode d'analyse du risque et les critères d'acceptation du risque;

- S'assure que les ressources sont gérées conformément à la politique de sécurité de l'information;
- Prépare les documents de revues de direction;
- Propose au responsable de la sécurité de l'information, les mesures de contrôle à mettre en place;
- Gère la documentation du système de la gestion de la sécurité de l'information (SGSI);
- Améliore le système de la gestion de la sécurité de l'information (SGSI);
- Traite les non-conformités.

Le gestionnaire

- Informe son personnel et, le cas échéant, tout intervenant externe, de la présente politique sur la sécurité de l'information et s'assure de son respect;
- Gère les droits d'accès de ses employés aux locaux et, le cas échéant, aux systèmes, aux bases de données, aux courriels, aux services Internet, à l'intranet, et ce, en fonction de leurs tâches;
- Participe au maintien du registre des incidents en déclarant au responsable de la sécurité de l'information tout incident de sécurité porté à sa connaissance;
- Collabore avec le responsable de la sécurité de l'information aux campagnes de sensibilisation de la sécurité de l'information;
- À titre de propriétaire des actifs informationnels :
    - assure une protection adéquate des informations et des processus d'affaires qui lui sont confiés;
    - établit les règles d'attribution et de retrait des droits d'accès aux informations qui sont sous sa responsabilité, s'assure de leur respect et, si nécessaire, autorise toute exception;
    - applique des mesures de contrôles lors de l'utilisation de l'information par les personnes autorisées à y accéder;

- catégorise les informations et les processus d'affaires sous sa responsabilité en fonction de la disponibilité, de l'intégrité et de la confidentialité;
- doit connaître les risques de sécurité de l'information des processus d'affaires sous sa responsabilité;

- Participe à l'élaboration des politiques, directives et éléments de gouvernance en matière de sécurité de l'information;
- Collabore à l'élaboration et à la mise à jour du registre d'autorité;
- Prend connaissance des événements consignés dans le registre des incidents le concernant, les analyse et formule les recommandations.

L'employé

- Prend connaissance et se conforme à la politique de la sécurité de l'information. Dans l'éventualité où un employé a une raison valable d'y déroger, il doit en aviser préalablement son gestionnaire afin d'obtenir une autorisation écrite;
- Accède à l'information exclusivement dans le cadre de ses fonctions;
- Limite l'utilisation des actifs informationnels aux fins pour lesquelles ils sont destinés;
- Signale sur-le-champ à son gestionnaire toute atteinte ou tentative d'atteinte à la sécurité de l'information telle que le vol, l'intrusion dans un système, l'utilisation abusive, la fraude, etc., dont il a connaissance.

8.2 Responsabilités des services et bureaux

Le Bureau du vérificateur général

- Effectue des examens de conformité indépendants et objectifs de l'efficacité des contrôles qui s'inscrivent dans les activités de la protection des actifs informationnels dans un contexte de gestion des risques;

- S'associe au processus du système de gestion de la sécurité de l'information afin d'en assurer l'audit de conformité indépendant;

- S'assure que les mesures de protection implantées garantissent une utilisation optimale et sécuritaire des actifs informationnels, dans le cadre d'un audit indépendant;

- Peut faire des recommandations au Comité de sécurité de l'information en matière de sécurité physique, logique, opérationnelle et documentaire afin de protéger les actifs informationnels, s'il y lieu;

- Peut prendre connaissance des événements consignés dans le registre des incidents, les analyse et formule des recommandations;

- Effectue le suivi des recommandations et des mesures correctives retenues.

Le Service des achats et de la gestion contractuelle

- Prévoit dans les contrats et les documents d'appel d'offres, une clause obligeant tout tiers contractant avec la Ville de respecter les exigences de la politique de sécurité de l'information.

Le Service du greffe

- Veille à l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
- Agit comme répondant, tant au sein de la Ville qu'auprès de la Commission d'accès à l'information, en ce qui concerne l'accès aux documents et la protection des renseignements détenus par la Ville;
- Coordonne et supervise la mise en œuvre de la Politique de gestion intégrée des documents;
- Collabore à l'élaboration et à la mise à jour de la matrice de catégorisation et du registre d'autorité;
- Prend connaissance des événements concernant ses champs d'expertise consignés dans le registre des incidents, les analyse et formule des recommandations.

Le Service de protection des citoyens

- Veille à l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* en agissant comme répondant en ce qui concerne l'accès aux documents et la protection des renseignements qu'il détient en tant que corps de police et en matière de sécurité incendie;
- Agit à titre de ressource dans des situations de soutien pour la protection des biens appartenant à Ville de Laval;
- Identifie les pratiques de sécurité à mettre en place pour l'habilitation sécuritaire du personnel et des utilisateurs et en assure l'application;
- Est responsable de la réalisation des enquêtes pour l'habilitation sécuritaire;
- Est responsable de la sécurité civile dans le cas de sinistres majeurs;
- S'assure de la continuité des activités pendant tout sinistre et de la reprise des activités normales après le sinistre. Cette responsabilité englobe le plan de continuité de l'organisation.

Le Service des ressources humaines

- Mentionne les responsabilités de l'employé en matière de sécurité avant l'embauche, dans des descriptions de poste adéquates, puis dans le contrat de travail;
- Assure de façon continue la formation et la sensibilisation de l'ensemble du personnel à la sécurité des actifs informationnels, l'informe des conséquences d'une atteinte à la sécurité ainsi que des rôles et des obligations de tous dans le processus de la sécurité et de la protection de l'information;
- Définit le processus disciplinaire des employés relativement aux infractions à la politique de sécurité de l'information;
- S'assure, lors du départ d'un employé, que son droit d'accès aux actifs informationnels prenne fin.

Le Service des systèmes et des technologies

- Veille au maintien de la sécurité des technologies supportant l'information numérique;
- Assure la gestion des processus de contrôle d'accès à l'information numérique;
- Assiste les propriétaires des actifs informationnels dans la mise en place et le maintien d'un environnement sécuritaire d'exploitation des systèmes dont ils sont responsables;
- Assure l'implantation des composantes technologiques afin de sécuriser l'information durant tout son cycle de vie. Il intervient également dans la conception, l'entretien et la continuité des systèmes en développement ou en exploitation ainsi qu'à la sécurité de l'infrastructure technologique partagée de la Ville;
- Assure la sécurité des technologies de l'information (techniques et logiques);
- Assure aux propriétaires des actifs informationnels la disponibilité, l'intégrité, la confidentialité, l'authenticité, l'irrévocabilité de l'information sous sa forme numérique selon les exigences et les droits d'accès définis par les propriétaires des actifs informationnels;
- Assure l'intégration harmonieuse des orientations et des exigences en matière de sécurité de l'information et de la protection des renseignements personnels au cours de la conception, de la réalisation ou de l'entretien de processus d'affaires, des systèmes d'information et des infrastructures technologiques;
- Informe et conseille les propriétaires des actifs informationnels et toute personne physique ou morale qui, par engagement contractuel ou autre, accèdent aux actifs informationnels numériques concernant les stratégies à mettre en œuvre, traite et élabore des solutions de sécurité associées à leurs demandes de développement de systèmes d'information;
- Identifie et gère les risques d'atteinte à l'intégrité des actifs informationnels numériques;
- Fournit aux propriétaires des actifs informationnels numériques le soutien, les outils et les conseils en matière de protection des actifs informationnels numériques;
- Collabore à l'élaboration et à la mise à jour de la matrice de catégorisation et du registre d'autorité;

- Prend connaissance des événements concernant ses champs d'expertise consignés dans le registre des incidents, les analyse et formule des recommandations;
- Surveille les systèmes et les journaux d'activités;
- Assure la sauvegarde et la récupération des données.

Le Service des travaux publics

- Identifie des mesures de sécurité physique des lieux et des personnes ainsi que des mesures de contrôle d'accès physique aux immeubles de la Ville et veille à leur mise en place;
- Procède, en collaboration avec le responsable de la sécurité de l'information, à l'analyse formelle et systématique des événements touchant la sécurité physique ayant mis ou qui aurait pu mettre en péril la sécurité de l'actif informationnel.

9. Entrée en vigueur, évaluation et modification

La présente politique entre en vigueur à la date de son approbation par le Conseil municipal.

La politique est évaluée annuellement afin de tenir compte des nouveaux besoins, des nouvelles pratiques et technologies, des nouvelles menaces et risques encourus.

Toute modification à la présente politique doit être approuvée par le Conseil municipal.