CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

Décembre 2019

LAVAL

TITRE Cadre de gestion de la sécurité de l'information	**Nº DE CONTRÔLE**
DIVISION PRINCIPALE Service de la sécurité de l'information / Service de l'innovation et des technologies	**ÉMISE LE** 2019-07-03
PROPRIÉTAIRE DU CADRE DE GESTION Amar Haicheur	**En vigueur depuis** 2019-07-03

Table des matières

1. Objectif

Le présent cadre vient en complément de la Politique de sécurité de l'information adoptée par la Ville et s'appuie aussi sur les directives complémentaires à la Politique. Il vise notamment à renforcer la gouvernance de la sécurité de l'information de la Ville par la mise en place d'une structure fonctionnelle de la sécurité de l'information, et à définir les rôles et les responsabilités à tous les niveaux de l'organisation.

Ce cadre de gestion permettra une mise en œuvre efficace et coordonnée des activités en matière de sécurité de l'information : la stratégie, la gestion des risques concertée, la reprise après sinistre ainsi que le respect de la conformité. L'éventail de ce cadre de gestion couvre la planification, la préparation de la mise en place, la mise en place ainsi que l'opérationnalisation de la sécurité. La rétroaction et l'amélioration continue sont aussi prises en considération dans ce cadre de gestion, de façon à limiter les impacts et les risques de potentiels dysfonctionnements pouvant porter atteinte à la prestation de services aux citoyens. L'application du cadre s'applique à la Ville de Laval ainsi qu'à tout partenaire, fournisseur ou sous-traitant qui livre des services au nom et pour la Ville de Laval.

2. Champ d'application

Le champ d'application du présent cadre est celui de la Politique de sécurité de l'information de la Ville de Laval.

3. Définitions

Actif informationnel : une information, quel que soit son canal de communication ou son support, une plateforme technologique et une solution d'affaires en technologies de l'information (TI) ou une TI, une installation ou un ensemble de ces éléments, acquis ou constitué par la Ville et sous sa responsabilité.

Confidentialité : propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

Continuité des services : capacité de la Ville d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

Cycle de vie : ensemble des étapes que franchit l'information (de sa création ou de 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).

Détenteur d'actif informationnel : gestionnaire à qui est assignée la responsabilité de la sécurité de l'information, d'une TI ou d'un processus d'affaires. L'emploi de ce terme ne signifie pas que la personne jouit de droits de propriété sur l'actif informationnel.

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

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.

Gouvernance de sécurité : validation des activités, des fonctions, des rôles et des processus ainsi que des relations établies entre ces derniers pour une saine gestion de la sécurité de l'information.

Information confidentielle : information appartenant ou relative à la Ville et qui n'a pas fait l'objet d'une annonce officielle par les autorités compétentes de la Ville ou dont le caractère confidentiel est conféré par une loi.

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

Intégrité : propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité; l'intégrité fait référence à l'exactitude et à la complétude.

Plateforme technologique : environnement hébergeant, d'un point de vue technique, une ou plusieurs composantes matérielles et logicielles afin d'offrir une prestation de services en TI soutenant une ou des solutions d'affaires en TI.

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

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 et d'identifier les mesures mises en place pour corriger la situation et éviter qu'elle ne se reproduise.

Registre des risques en TI : registre permettant de recueillir tous les risques inhérents, leur probabilité, les mesures d'atténuation ainsi que le seuil d'acceptation pour chacun d'entre eux.

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 (SI) : état de protection des actifs informationnels face aux risques identifiés, qui 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.

Solution d'affaires en TI : ensemble d'application et de services en TI combinés afin d'offrir une valeur d'affaires à un service ou à un bureau de la Ville ou aux citoyens pour répondre à un problème ou à un contexte d'affaires complexe à l'aide de technologies.

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.

Utilisateur : toute personne physique ou morale qui, par engagement contractuel ou autrement, fait usage ou a accès à tout actif informationnel sous la responsabilité de la Ville (ex : les employés, municipaux sans égard à leur catégorie d'emploi ou à leur statut, les citoyens, les élus, les fournisseurs, les partenaires ainsi que toute personne ayant recours aux services de la Ville).

4. Cadre légal

Le cadre de gestion s'inscrit dans un contexte régi par le cadre légal et administratif défini au sein de la Politique de sécurité de l'information adoptée par la Ville.

Une liste de ces lois et de ces règlements est présentée en annexe II de la Politique de sécurité de l'information.

5. Rôles et responsabilités

5.1. Structure des comités

5.1.1. Conseil municipal

- Approuve les orientations générales soumises par le comité exécutif en matière de sécurité de l'information;
- Adopte tout changement à la Politique de sécurité de l'information à la suite des recommandations du comité exécutif.

5.1.2. 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.

5.1.3. 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'une attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information;
- Fournit les ressources nécessaires pour soutenir les initiatives de sécurité.

5.1.4. Comité de sécurité de l'information

Sous l'autorité du comité exécutif et de la direction générale, ce comité contribuera aux différents volets de responsabilités :

- La stratégie de gestion de la sécurité de l'information;
- La gestion des risques;
- La reprise après sinistre;
- La conformité.

Les actions du comité portent sur l'ensemble des services et des bureaux de la Ville de Laval; ces derniers sont assujettis aux recommandations du comité de sécurité de l'information. Toute action demandée par ce comité doit être reçue et exécutée. Le comité fera un suivi des plans d'action.

Le comité communiquera aux différentes instances les résultantes émanant de ces rencontres pour lesquelles des actions pourraient être requises par différents groupes.

Ce comité peut aussi, au besoin :

- Convoquer les intervenants en audience;
- Réquisitionner le soutien de ressources additionnelles.

5.1.4.1. Stratégie de gestion de la sécurité de l'information

- S'assure que la Politique de sécurité de l'information et les directives répondent aux objectifs et à la stratégie de l'organisation;
- Agit comme conseiller et influence les orientations de la direction générale pour tenir compte de la sécurité de la gestion 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;
- S'assure de communiquer les approches à suivre en ce qui concerne les mesures à mettre en place;
- Représente la Ville auprès des autres municipalités et instances en matière de sécurité de l'information.

5.1.4.2. Gestion des risques en TI

- Assure une gouvernance sur les risques en technologies de l'information et sur la sécurité des actifs informationnels, incluant l'évaluation des impacts potentiels ainsi que les mesures d'atténuation qui s'appliquent;
- Approuve les critères d'acceptabilité des risques et des risques résiduels;
- Valide l'état du registre des risques de façon récurrente;
- S'assure de communiquer les attentes aux différents groupes en matière de gestion des risques.

5.1.4.3. Reprise après sinistre

- Valide à ce que les exercices de reprise après sinistre soient faits annuellement;
- S'assure du bon fonctionnement des processus entourant la reprise après sinistre (incluant que les mises à jour soient faites dans tous les systèmes actifs et passifs);
- S'assure que la documentation qui permet de mettre en place la reprise après sinistre est à jour;
- S'assure que les plans de reprise après sinistre sont mis en œuvre;
- S'assure que les ressources participant au plan de reprise après sinistre sont nommées et reconfirmées périodiquement; ces ressources doivent avoir été informées de leur rôle et de ce qui est attendu d'eux;
- Déclenche le processus de gestion de continuité des opérations et de relève;
- S'assure qu'un plan de communication est établi et livré dans le cadre d'une reprise après sinistre.

5.1.4.4. Conformité

- Recommande les dossiers pour analyse au Bureau d'intégrité et d'éthique de Laval (BIEL) dans ses champs de compétence;
- Approuve les politiques et les directives de sécurité;
- Revoit, au besoin, l'interprétation qui est faite de la Politique et des directives de sécurité;
- S'assure de la persistance et de la cohérence entre les documents formels, comme les politiques et les directives, et recommande la revue des guides et des instructions de travail de façon à ce qu'ils respectent les changements qui peuvent être apportés aux politiques et aux directives de sécurité;
- S'assure de revoir l'arrimage avec les législations en matière de protection des renseignements personnels et de sécurité de l'information;
- S'assure que la sensibilisation des utilisateurs est faite par tous les groupes selon les calendriers de révision prévus;
- Réquisitionne les audits de sécurité internes et externes périodiquement;
- Effectue le suivi des plans d'action en sécurité de l'information à tous les niveaux;

- S’assure de pouvoir revoir les incidents de sécurité (*post-mortem*) et de valider les propositions de plans d’action qui porteront à la fois sur la technologie, les comportements et les processus;
- Revoit tous les aspects relatifs à l’accès aux documents, à la protection des renseignements personnels et à la sécurité de l’information;
- S’assure d’avoir un plan de communication pour faire face aux différentes situations au regard de la conformité;
- S’assure de la considération des impacts des changements législatifs.

5.1.4.5. Composition du comité

- Un membre de la gestion de la direction générale;
- Un membre de la gestion du Service du greffe;
- Un membre de la gestion du Service des affaires juridiques;
- Un membre de la gestion du Service des ressources humaines;
- Un membre de la gestion du Service des communications et du marketing;
- Un membre de la gestion du BIEL et du Service de police de Laval;
- Un membre de la gestion du Service de la gestion des immeubles;
- Un membre de la gestion des services critiques (Eau);
- Le directeur du Service de l’innovation et des technologies;
- Un membre de la gestion du Service de l’innovation et des technologies pour la reprise après sinistre.

5.1.5. Comité de gestion de crise en cybersécurité

Le comité de cybersécurité peut, à tout moment, activer la cellule de crise (comité de gestion de crise). Ce dernier est formé des intervenants clés qui ont la responsabilité de déclencher le processus menant à la continuité opérationnelle et à la relève informatique. Ce comité :

- Coordonne les activités de retour à la normale avec différents services, notamment les suivants :
  - Sécurité civile (sécurité physique et des personnes);
  - Direction générale (autorité et coordination des services et des bureaux);
  - Service de l’innovation et des technologies;
  - Service des communications et du marketing;
- 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.

Notez que ce comité ne se substitue pas aux comités qui sont mis en place par la Sécurité civile; il y a peut-être des intégrations à prévoir dans le plan global de la Ville.

5.1.6. Comité d'architecture

Dans un contexte de sécurité, en plus de ses tâches de gouvernance en architecture, le comité :

- Approuve les normes et les standards de sécurité qui doivent être pris en considération dans la mise en place des architectures;
- Approuve les composantes de sécurité des architectures de solutions;
- Assure le suivi des demandes de corrections en architecture pour la sécurité;
- Autorise la mise en œuvre et l'exploitation de services de sécurité à titre de fondations en sécurité de l'information.

5.1.7. Comité de sécurité opérationnelle

Dans le contexte de revue des incidents, le comité de sécurité opérationnelle accomplit les activités suivantes :

- S'assure que les solutions sont implantées de façon sécuritaire, conformément aux architectures, et qu'elles sont documentées au moyen d'instructions de travail conformes;
- S'assure que les solutions sont opérationnalisées selon les prescriptions d'architecture (standards), de façon à couvrir le fonctionnement normal et la relève;
- Revoit les incidents de sécurité, explique les impacts et propose des mesures d'atténuation de façon à réduire les risques;
- Exploite la gestion de la sécurité de l'information au quotidien.

5.2. Rôles et responsabilités des bureaux et services

5.2.1. 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;
- Implique l'architecture pour la définition des aspects technologiques en sécurité de l'information pour les solutions et les services à définir.

5.2.2. 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.

5.2.3. Service de sécurité publique

- 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 la Ville de Laval;
- Détermine les pratiques de sécurité à mettre en place pour l'habilitation de sécurité du personnel et des utilisateurs et en assure l'application;
- Effectue les enquêtes pour l'habilitation de sécurité;
- Prend en charge la sécurité civile dans le cas de sinistres majeurs.

5.2.4. Service des travaux publics

- Détermine les mesures de sécurité physiques des lieux et des personnes ainsi que les 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.

5.2.5. Service de l'innovation 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 solutions d'affaires dont ils sont responsables;
- Assure l'implantation des composantes technologiques afin de sécuriser l'information durant tout son cycle de vie;
- Intervient dans la conception, l'entretien et la continuité des solutions d'affaires en développement ou en exploitation ainsi que dans 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 et 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 solutions d'affaires 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 livraison de solutions d'affaires;
- Cerne et gère les risques d'atteinte à l'intégrité des actifs informationnels numériques;
- Fournit aux propriétaires des actifs informationnels numériques du soutien, des outils et des conseils en matière de protection des actifs informationnels numériques;
- Collabore à l'élaboration et à la mise à jour de la matrice de catégorisation des actifs informationnels;
- Prend connaissance des événements concernant ses champs d'expertise consignés dans le registre des incidents, les analyse et formule des recommandations;
- Surveille les écosystèmes et les journaux d'activités;
- Assure la sauvegarde et la récupération des données.

5.2.6. Service des ressources humaines

- S'assure que les employés ont reçu les instructions pour se conformer à la Politique et aux directives de sécurité;
- Contrôle le registre de suivi de sensibilisation sur la Politique et les directives de sécurité des employés;
- Réitère l'importance de la sensibilisation sur la Politique et les directives de sécurité auprès des gestionnaires;
- Communique les responsabilités de l'employé en matière de sécurité de l'information et des actifs informationnels avant la signature de la lettre d'embauche;
- Assure de façon continue la formation et la sensibilisation de l'ensemble du personnel à la sécurité des actifs informationnels en expliquant, entre autres, les conséquences d'une atteinte à la sécurité ainsi que les rôles et les obligations;
- 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 a pris fin.

5.2.7. Pour tous les services et bureaux

5.2.7.1. Gestionnaire

- Informe son personnel et, le cas échéant, tout intervenant externe de la présente Politique sur la sécurité de l'information et des recommandations du comité de sécurité, et s'assure de son respect;
- Gère les droits d'accès de ses employés aux locaux et, le cas échéant, aux solutions d'affaires, aux courriels, aux services Internet et 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 contrôle lors de l'utilisation de l'information par les personnes autorisées à y accéder.

5.2.7.2. Employé

- Prend connaissance et se conforme à la Politique et aux directives de sécurité de l'information;
- S'assure de suivre le calendrier de sensibilisation à la sécurité des actifs informationnels;
- 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 ou autre dont il a connaissance.

5.3. Officier de sécurité (CISO)

L'officier de sécurité est sous l'autorité du directeur du Service de l'innovation et des technologies.

5.3.1. Stratégie de sécurité

- 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;
- 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 tout au long du cycle de vie de l'information (collection, utilisation, conservation, communication, élagage et destruction);
- Fait approuver – par le comité de sécurité de l'information – les documents et les activités du plan d'action stratégique en sécurité de l'information et ceux ayant une incidence tactique ou opérationnelle;
- 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;
- Prépare les documents de revues pour le comité de sécurité.

5.3.2. Gestion des risques en TI

- Définit la méthode d'analyse du risque et les critères d'acceptation des risques;
- S'assure de l'identification et de la gestion des risques d'atteinte à la sécurité de l'information et cerne les risques résiduels qui doivent être assumés par le comité de sécurité de l'information et lui transmet 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;
- S'assure, dans le cadre d'un audit indépendant, que les mesures de protection implantées garantissent une utilisation optimale et sécuritaire des actifs informationnels;
- 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 a lieu.

5.3.3. Reprise après sinistre

- Élabore, met en place et maintient à jour le plan de reprise après sinistre des actifs informationnels et des processus d'affaires critiques désignés par les propriétaires des actifs informationnels;
- S'assure que tous les services sont couverts par un plan pour la reprise après sinistre (y compris pour les nouvelles solutions déployées).

5.3.4. Conformité

- Gère l'implantation de la Politique de sécurité de l'information;
- S'assure que la sensibilisation du personnel, des gestionnaires et de toute personne utilisant ou accédant aux informations appartenant à la Ville et à ses citoyens est réalisée de façon périodique;
- S'assure du respect de la Politique et des directives de sécurité de l'information;
- Soutient le rôle du Service du greffe au regard des obligations et des pratiques en matière d'accès à l'information, de la protection des renseignements personnels et de la sécurité de l'information;
- S'assure que la matrice de catégorisation est maintenue à jour.

5.3.5. Opérationnel

- Assure la cohérence et la pertinence des interventions en matière de sécurité de l'information;
- S'assure que les ressources sont gérées conformément à la Politique et aux directives de sécurité de l'information;
- S'assure de la création et du maintien du registre des incidents de sécurité ainsi que du suivi des mesures correctives;
- Peut prendre connaissance des événements consignés dans le registre des incidents, les analyser et formuler des recommandations;
- Peut être appelé à témoigner au tribunal en cas de poursuite;
- Contribue au comité de sécurité opérationnel en tant qu'expert.

6. Approbation et version

RESPONSABLE DU CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION	SIGNATURE
TITRE	DATE D'APPROBATION

Version	Rédacteur	Commentaires/mises à jour	Date
1.0	Helene C Decelles	Version initiale	2019-06-21
1.1	Joel Moreault	Ajustement - commentaires CEO	2019-07-03

Production : Ville de Laval — COM-12-19

RESTEZ INFORMÉS !

Pour des informations générales, visitez notre site Web :

laval.ca

Par téléphone
311 ou
450 978-8000
(de l'extérieur de Laval)

En personne
Comptoir multiservice
1333, boulevard Chomedey