POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Préparée par :
Le Service des technologies de l'information

Version : 1.0
Mise à jour date : 2018-10-31
Audience : Ville de Québec
Portée de la politique : Ville de Québec

Catégorisation du document : D-1, I-2, C-1

Table des matières

1. Contexte

La Ville de Québec (ci-après « Ville ») a entre autres pour objectif d'offrir aux citoyens des services performants, de qualité et accessibles. Dans le cadre de sa mission, la Ville détient des informations de nature sensible. Elle doit conséquemment, dans le cadre légal qui lui est applicable, assurer la confidentialité de ces informations afin, notamment, de protéger les citoyens. L'information qu'elle détient possède une valeur légale, administrative, économique ou patrimoniale qu'il convient de gérer et de protéger adéquatement durant tout son cycle de vie.

L'indisponibilité, un manque d'intégrité ou la divulgation inappropriée (confidentialité) de l'information peut notamment générer des impacts graves allant jusqu'à mettre en péril le fonctionnement de services essentiels, entraîner des pertes financières importantes, miner la réputation de la Ville ou encore, menacer la vie privée, la santé ou la sécurité des personnes.

Il convient de mettre en œuvre un ensemble cohérent de mesures visant à assurer une protection adéquate des actifs informationnels (ci-après « AI »). Ces mesures doivent prendre en compte la valeur de l'information et aussi les obligations de la Ville. L'information doit être protégée par des mesures appropriées durant tout son cycle de vie, de sa création jusqu'à sa disposition.

2. Objectifs de la politique

La présente politique et les documents d'encadrement de la sécurité expriment la vision de la Ville quant à l'importance stratégique de protéger ces AI qui ont un impact direct sur sa mission, sa crédibilité, le maintien ou le rehaussement de ses relations de confiance avec ses citoyens, ses fournisseurs, ses partenaires et son personnel. Elle contribue aussi au respect des obligations légales de la Ville incluant notamment la protection des renseignements personnels (ci-après « PRP ») et la protection de la vie privée. Cette politique constitue la pierre d'assise qui énonce les orientations et les principes directeurs en matière de gestion de la sécurité de l'information. Elle vise l'amélioration continue de la sécurité de l'information conformément aux objectifs d'affaires de la Ville pour assurer la disponibilité, l'intégrité, la confidentialité des AI.

La politique comprend les éléments suivants :

2.1. L'assurance d'une culture de sécurité de l'information

La Ville accorde une importance au respect du caractère confidentiel de l'information, de la vie privée, du secret industriel, de la propriété intellectuelle et à la PRP. Le renforcement et le maintien d'une culture en matière de sécurité de l'information permettront de renforcer la confiance des différents acteurs.

De plus, plusieurs des processus d'affaires supportés par la Ville nécessitent que l'information utilisée par ces derniers soit complète, exacte et disponible en temps opportun.

2.2. L'attribution de responsabilités à chaque utilisateur

La préoccupation à l'égard de la sécurité de l'information et de la PRP doit être partagée par les utilisateurs des AI de la Ville. Cela exige l'attribution claire de responsabilités à tous les paliers de l'organisation afin d'assurer une gestion sécuritaire de l'information et de permettre une reddition de compte adéquate.

2.3. La concertation des acteurs et de la gestion selon une approche globale

L'efficacité et l'efficience de la sécurité de l'information reposent sur une approche globale qui tient compte de l'ensemble des composantes de l'organisation, tels les aspects juridiques, humains, éthiques, financiers, organisationnels et technologiques. Cela requiert la concertation à tous les niveaux de l'organisation afin d'assurer la cohérence des interventions et l'optimisation des ressources.

2.4. Les assises nécessaires au respect des lois et règlements

La conformité aux lois et règlements applicables ainsi que les directives, normes et orientations et bonnes pratiques sont essentielles afin d'assurer une saine gestion de la sécurité de l'information.

3. Champ d'application

3.1. Cette politique s'applique à :

Tout employé ou bénéficiaire de services de la Ville qui utilise ou peut avoir accès à un ou plusieurs AI, peu importe l'endroit où il se trouve ou la localisation de l'AI.

Tout consultant, fournisseur, partenaire, ou organisme appelé à accéder ou à utiliser les AI de la Ville.

3.2. L'information visée par la présente politique est :

Celle que la Ville de Québec détient dans l'exercice de sa mission, que sa conservation soit assurée par elle-même ou par un tiers, soit, entre autres :

- Les AI appartenant à la Ville et exploités par elle;
- Les AI appartenant à la Ville et exploités ou détenus par un partenaire, un fournisseur de produits et de services ou un autre intervenant;
- Les AI appartenant à un partenaire, à un fournisseur de produits et de services, ou un autre intervenant, et exploités par lui au profit de la Ville;
- Les AI n'appartenant pas à la Ville et détenus par elle.

3.3. Activités visées par la politique :

Sous réserve de toute disposition législative à l'effet contraire, cette politique s'applique à toute activité impliquant l'utilisation, la transmission ou la conservation, sous quelque forme que ce soit, d'un AI appartenant à la Ville, ou détenu par elle, sans égard aux supports ou aux emplacements, qu'elle soit exercée dans les locaux de cette dernière, ou un autre lieu, tout au long du cycle de vie de cet AI.

4. Définitions

Les définitions font partie de cette politique et sont indiquées à **l'annexe II**.

5. Cadre légal et administratif

Le volet légal influence la gestion de la sécurité de l'information. Les lois et les règlements prescrivent des exigences de sécurité de l'information auxquelles la Ville doit s'astreindre.

La politique doit être appliquée et interprétée en fonction des lois en vigueur au Québec et au Canada, des lois d'autres pays, lorsque requis, des ententes ou contrats avec des tiers, ainsi que des conventions collectives et des protocoles établissant les conditions de travail de certaines catégories de personnel. Les lois et règlements de portée générale ou sectorielle doivent également être pris en compte.

6. Principes directeurs

La Ville reconnaît que l'information ainsi que les technologies permettant de la traiter sont essentielles à la réalisation de sa mission et de ses activités. Elles doivent faire l'objet d'une protection proportionnelle à la sensibilité de l'information, aux risques auxquels elle est exposée et aux impacts anticipés en cas d'incident. Les protections sont réévaluées régulièrement pour tenir compte des changements et de l'évolution des menaces et des risques.

En ce sens, la Ville s'engage à ce que les solutions retenues correspondent aux bonnes pratiques en matière de sécurité de l'information, tant sur le plan national que sur le plan international.

Les principes directeurs s'appuient sur les objectifs de la politique. Ils constituent les exigences de base auxquelles toute personne ou entité assujettie à la politique doit se conformer. Ils doivent être pris en compte dans la gouvernance, la gestion et les opérations de la Ville.

6.1. Planifier la protection de l'information pour tout son cycle de vie

Le choix des mesures de sécurité s'appuie sur l'évaluation des risques affectant l'information. En particulier, la catégorisation de l'information, l'évaluation des risques et la définition des exigences de sécurité doivent être réalisées dès les premières phases des travaux et ce jusqu'à la fin de ces derniers.

6.2. Catégoriser les ressources informationnelles

Toute ressource informationnelle fait l'objet d'une identification et d'une catégorisation selon un processus commun d'évaluation qui permettra d'en définir la valeur en matière de disponibilité, d'intégrité et de confidentialité. Elle est formellement assignée à un détenteur ou gestionnaire qui en est responsable.

6.3. Évaluer les risques

Toute ressource informationnelle fait l'objet d'une analyse de risques selon un processus commun d'évaluation en ce qui a trait à la protection de l'information. Une évaluation des risques est aussi réalisée dès les premières phases d'un projet ou d'un changement majeur (acquisition, développement ou une impartition d'un AI, etc.). Les risques sont consignés dans un registre (outil permettant de colliger les risques) afin d'en faciliter la gestion.

6.4. Mettre en place les mesures de protection appropriées

Les mesures de protection sont définies de façon proportionnelle à la valeur de l'actif et aux risques auxquels il est soumis. Les mesures de protection appropriées doivent être appliquées tout au long du cycle de vie de l'information de la Ville, c'est-à-dire, dès sa création en passant par son enregistrement, son transfert, sa consultation, son traitement, son utilisation, sa transmission et sa conservation, jusqu'à sa destruction. La valeur et la sensibilité de l'information, les risques et, conséquemment, les mesures de sécurité peuvent varier durant le cycle de vie.

La Ville peut notamment procéder à des contrôles de tout équipement informatique, du matériel électronique, des informations qu'ils supportent, des téléchargements, des sites Internet visités et, dans certaines circonstances, du courrier électronique, utilisant ou connecté aux actifs informationnels de la Ville.

Chaque utilisateur doit être associé à un compte unique afin d'être en mesure de suivre son parcours au travers des systèmes d'information de la Ville. Par conséquent, l'utilisation de compte générique est à proscrire, mais des exceptions pourront être autorisées, par l'équipe de sécurité, selon le besoin.

Tous les comptes des utilisateurs doivent nécessiter un mot de passe qui répondra aux exigences minimales de sécurité définies par l'équipe de sécurité de la Ville.

6.5. Gestion des environnements et maintenance

Seul un personnel habilité et autorisé par le Service des technologies de l'information peut procéder à la maintenance des systèmes informatiques de la Ville. L'environnement servant à effectuer la maintenance des systèmes doit être isolé de l'environnement de production.

L'acquisition, le développement et la maintenance des applications doivent être associés à des processus formels contrôlés par le Service des technologies de l'information.

Les systèmes associés aux informations critiques de la Ville, ne doivent être accessibles que par l'intermédiaire de moyens sécurisés dans un environnement contrôlé et restreint.

Les informations numériques, les systèmes associés, procédures et documentation doivent faire l'objet d'une sauvegarde appropriée pour répondre aux critères de disponibilité, d'intégrité et de confidentialité déterminés par son détenteur.

Toute opération critique effectuée sur ou par les systèmes d'informations jugés sensibles par les détenteurs d'actifs doit pouvoir être associée à des journaux d'événements correctement sécurisés et préservés pour références futures.

Les ententes et les contrats de la Ville (l'acquisition, le développement et la maintenance des applications) doivent contenir des dispositions garantissant le respect des standards de sécurité de l'information de la Ville.

6.6. Suivre le processus formel de gestion des changements organisationnels - volet sécurité

Les processus en place pour la gestion des changements et des mises en production du Service des technologies de l'information doivent être respectés quant à la gestion des risques et au volet sécurité.

6.7. Protéger les renseignements confidentiels

La Ville détient des données à caractère confidentiel notamment des renseignements personnels. Conséquemment des mesures doivent être prises afin d'encadrer les risques reliés à ces données.

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « *Loi sur l'accès* ») impose des obligations particulières pour les renseignements personnels. Ces derniers doivent être à jour, exacts et complets pour servir aux fins prévues. Sous réserve des lois applicables, il faut en disposer lorsque les fins pour lesquelles ils ont été recueillis ou utilisés sont accomplies en respect de la vie privée des individus. La Ville applique, sans s'y limiter, les principes suivants :

- limiter la **collecte** des renseignements à ceux qui sont nécessaires;
- veiller à ce que les renseignements qu'elle détient soient **exacts et à jour**;
- **utiliser** les renseignements uniquement aux fins pour lesquelles ils ont été recueillis et ne les conserver que le temps nécessaire aux fins pour lesquels ils sont recueillis;
- **restreindre** les accès aux seules personnes ayant besoin de ces renseignements dans l'exercice de leur fonction;
- **transmettre ces renseignements suite au consentement** de la personne concernée ou en conformité avec la *Loi sur l'accès*. En l'absence d'un tel consentement, prendre les mesures nécessaires, pour préserver la confidentialité de l'information lors de sa transmission.

Tout support contenant de l'information confidentielle doit être conservé de façon sécuritaire. L'information confidentielle doit être détruite de façon irréversible lorsque sa détention ou son utilisation n'est plus nécessaire, en conformité avec le calendrier de conservation, ou lorsque le support est mis au rebut ou utilisé à d'autres fins.

6.8. Préserver l'intégrité, la valeur probante et juridique de l'information

L'intégrité de l'information doit être maintenue à un niveau adéquat en fonction de la catégorisation, des besoins d'affaires ainsi que des obligations légales et contractuelles. Plus particulièrement, la Ville doit préserver la valeur probante de l'information durant tout son cycle de vie nonobstant les changements de format ou de support, afin de préserver son admissibilité potentielle devant les tribunaux.

À cette fin, les processus, procédés et mécanismes qui encadrent la copie, le classement, la saisie, la conservation, la journalisation, la transmission ou le transfert de l'information doivent assurer le maintien de son intégrité et, conséquemment, de sa valeur probante.

6.9. Assurer la disponibilité et la conservation de l'information

L'information doit être accessible et utilisable en temps voulu par les personnes autorisées. En conséquence, des mesures doivent être mises en place pour garantir le niveau de disponibilité requis.

La Ville est soumise à des règles en matière de gestion des documents actifs, semi-actifs et inactifs des organismes publics établies par la *Loi sur les archives* et le *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques*. En conséquence, il est nécessaire de planifier et de contrôler la création, l'utilisation, la conservation et la disposition finale de l'information en utilisant les moyens appropriés, selon la catégorisation de cette dernière. Pour ce faire, la Ville doit établir et tenir à jour un calendrier de conservation pour cette dernière.

De plus, la *Loi sur l'accès* impose notamment d'établir et de tenir à jour un plan de classification des documents. Cela implique la mise en place de mesures de sécurité.

6.10. Assurer la continuité des services municipaux et des opérations

La Ville planifie, avec la collaboration de différents intervenants internes et externes, un plan de continuité des affaires visant la remise en opération, dans un délai raisonnable, des services et processus d'affaires jugés essentiels ou stratégiques en cas de situation d'exception.

6.11. Assurer la mise en place des plans de relève informatique

Le responsable de la sécurité de l'information numérique (RSIN) planifie, avec la collaboration de la direction du Service des technologies de l'information et des différentes unités d'affaires de la Ville, des plans de relève informatique afin de s'assurer de la remise en opération des systèmes d'informations essentiels en cas de panne majeure et de la continuité des services. De plus, des mesures de relève doivent être testées et révisées lors d'importantes acquisitions affectant les ressources informationnelles ou lors de changement organisationnel.

6.12. Assumer la responsabilité au-delà du périmètre de la Ville

La sécurité de l'information de la Ville est une responsabilité partagée avec toutes les personnes qui utilisent les AI. Ainsi, chaque employé, consultant ou fournisseur de services doit protéger l'information mise à sa disposition en l'utilisant avec discernement et aux seules fins prévues dans le cadre de son travail ou de son mandat et en respectant les règles d'usage en vigueur.

Les ententes et les contrats avec les fournisseurs, partenaires et mandataires doivent contenir des dispositions garantissant le respect de cette politique.

Ces dispositions doivent inclure des clauses de sécurité quand le mandat confié requiert l'utilisation ou la transmission d'informations avec la Ville. Ces clauses doivent décrire, notamment, les responsabilités des parties ainsi que les mécanismes d'accès, de conservation et de transmission de l'information.

6.13. Exercer un processus formel de gestion des identités et des accès

Les personnes autorisées à accéder à l'information jouent un rôle fondamental dans la sécurité de l'information. En conséquence, l'accès à l'information et aux AI est conditionnel à l'obtention d'une autorisation formelle. Cette autorisation est conditionnelle à des vérifications, notamment quant à l'identité des personnes à qui sont attribués les privilèges et à ceux qui leur sont consentis. Ces derniers varient selon la nature ou la sensibilité de l'information à laquelle une personne a accès.

La maintenance de toute application ou tout processus ne doit être confiée qu'à un personnel dûment habilité et autorisé par le responsable de la présente politique.

6.14. Respecter la propriété intellectuelle

La Ville respecte les exigences légales relatives à la propriété intellectuelle concernant l'utilisation de produits, documents, informations et brevets. Tout utilisateur doit également se conformer à ces exigences, que les droits de propriété intellectuelle appartiennent à la Ville ou non.

6.15. Utiliser de façon éthique les actifs informationnels

La Ville met à la disposition des utilisateurs des AI afin qu'ils puissent exercer les tâches reliées à leurs fonctions. Chaque utilisateur doit les utiliser avec vigilance en respectant les lois et règlements en vigueur au Québec et au Canada.

Les outils de télécommunications utilisant Internet (courriel, web, etc.) doivent être utilisés de façon éthique. Entre autres, ils ne doivent pas servir à transmettre des informations confidentielles et, si cela s'avère être le cas, l'utilisateur doit utiliser des moyens jugés sécuritaires et agir conformément aux prescriptions légales.

6.16. Utiliser adéquatement les outils personnels au travail

Les outils personnels, notamment les tablettes électroniques, les téléphones intelligents et les autres outils du même type ne peuvent être utilisés au travail à des fins professionnelles. Malgré cette règle, ils peuvent l'être s'ils ont été autorisés via une permission écrite du gestionnaire.

6.17. Auditer les actifs informationnels

La Ville emploie des outils de surveillance, de contrôle et d'enregistrement de toute utilisation de ses actifs informationnels et peut en tout temps analyser et évaluer l'usage qui en est fait.

Afin de permettre la détection de logiciels malveillants, la Ville peut surveiller tout trafic transitant par ses réseaux informatiques, incluant toutes les connexions chiffrées et ce, dans le respect des lois applicables. Ceci inclut la surveillance des services de courriels en ligne ainsi que tout autre service à usage personnel. Seuls certains sites jugés de confiance absolue sont exempts de ce type d'audit.

6.18. Utiliser le courrier électronique

Dans le but de lutter contre la propagation et l'exécution de codes malveillants, l'interception d'informations sensibles, la désinformation et la publication d'informations illégales, diffamatoires ou de harcèlement, la Ville établit les règles suivantes quant à l'utilisation de son service de courrier électronique. L'utilisateur :

- doit s'identifier à chacun de ses messages;
- doit respecter la confidentialité des messages et éviter d'intervenir sur tout message qui ne lui est pas destiné;
- doit éviter de surcharger le système de messagerie;
- ne doit pas capter, stocker, reproduire ou transmettre du matériel ou un message à caractère illégal;
- ne doit pas se servir de l'adresse de courriel ou de la messagerie électronique à des fins commerciales ou illicites;
- ne doit en aucune façon expédier, sans autorisation, à tous les employés de la Ville, des lettres en chaîne et toute information non pertinente aux activités de la Ville;
- **ne doit pas répondre ou ouvrir un courrier électronique** de provenance douteuse;
- **ne doit pas cliquer sur un lien** dont l'adresse de courrier électronique semble étrange;
- doit rédiger ses messages de courrier électronique avec le plus grand soin en employant, en toute circonstance, un langage professionnel.

6.19. Exercer un droit de regard et d'intervention

Afin de protéger l'information qu'elle détient, la Ville peut exercer un droit de regard et d'intervention sur l'utilisation qui en est faite et ce, pour quiconque y ayant accès, afin de s'assurer que cette dernière

est conforme aux lois et règles applicables, qu'il n'y a pas d'abus et que la sécurité et la performance de ses systèmes sont convenablement maintenues.

Ce droit de regard est exercé conformément au cadre légal et administratif applicable à la Ville,

6.20. Travailler à distance (télétravail)

Seules les personnes autorisées par leur gestionnaire à utiliser le télétravail ont des accès distants aux services ou aux logiciels nécessaires à leurs fonctions, selon des modalités précises définies par l'équipe de sécurité de la Ville et selon les termes prévus dans les conventions collectives. L'utilisateur doit respecter les ententes formelles établies à cet égard et les directives qui en découlent afin d'assurer le respect de la présente politique.

6.21. Responsabiliser et former

La Ville s'assure que son personnel reçoit de la formation qui vise entre autres à le sensibiliser et le responsabiliser face à la sécurité des AI, afin d'atteindre ses objectifs de sécurité quant à leurs rôles et obligations en la matière.

7. Rôles et responsabilités

La structure fonctionnelle de la sécurité de l'information et de la protection des renseignements confidentiels de la Ville ainsi que les rôles et responsabilités des principaux intervenants en sécurité de l'information et renseignements confidentiels sont décrits dans le cadre de gestion de la sécurité de l'information et de la PRP de la Ville. L'ensemble des rôles et responsabilités sont résumés dans un schéma inclus en annexe IV du présent document.

7.1. Conseil municipal

Le conseil municipal approuve la présente politique et les orientations générales soumises par le comité exécutif, en matière de sécurité de l'information. À la suite des recommandations du comité exécutif, le conseil municipal adopte tout changement à la politique de sécurité de l'information ayant un impact sur ses orientations générales.

7.2. Comité exécutif

Le comité exécutif recommande au conseil municipal l'adoption de la présente politique et les orientations générales en matière de sécurité de l'information. Il lui fait également un suivi sur leur mise en œuvre et leur application.

7.3. Directeur général

Le directeur général s'assure que les valeurs et les orientations en matière de sécurité soient partagées par l'ensemble des gestionnaires et du personnel de la Ville. Il s'assure de l'application de la politique dans l'organisation, apporte les appuis financiers et logistiques nécessaires pour la mise en œuvre et l'application de la présente politique. Il soumet le bilan annuel concernant l'application de la politique au comité exécutif. Il exerce son pouvoir d'enquête et applique les sanctions prévues à la présente politique, lorsque nécessaire.

7.4. Responsable de la sécurité de l'information numérique

À titre de représentant délégué du directeur général en matière de sécurité des AI, le responsable de la sécurité de l'information numérique, ci-après le RSIN, gère et coordonne la sécurité au sein de la Ville. Il doit donc superviser l'action des divers acteurs dans l'élaboration, la mise en place, le suivi et l'évaluation de la sécurité de l'information.

Entre autres :

- Il veille à l'élaboration et à l'application de la politique sur la sécurité de la Ville. Dans cette perspective, il collabore avec tous les gestionnaires;
- Il identifie les détenteurs d'actifs informationnels dans leur secteur respectif;
- Il s'informe des besoins en matière de sécurité auprès des détenteurs et des gestionnaires, leur propose des solutions et coordonne la mise en place de ces solutions;
- Il gère les aspects relatifs à l'escalade des incidents de sécurité;
- Il doit informer immédiatement le gestionnaire responsable, lorsqu'il constate qu'un utilisateur déroge à la présente politique;
- Il suit la mise en œuvre de toute recommandation découlant d'une vérification ou d'un audit;
- Il produit annuellement, et au besoin, pour la direction générale, les bilans et les rapports relatifs à la sécurité des actifs informationnels appartenant à la Ville.

7.5. Conseiller en sécurité de l'information

Le conseiller en sécurité de l'information, ci-après le COSI, apporte son soutien au RSIN au plan tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information. Au-delà de son rôle de soutien auprès du RSIN, le COSI est notamment chargé :

- De mettre en œuvre les orientations internes découlant des directives, des politiques internes et des pratiques généralement admises à cet égard;
- De produire les bilans et les plans d'action de sécurité de l'information;
- De participer aux négociations des ententes de service et des contrats et de formuler des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information;
- De tenir à jour le registre d'autorité de la sécurité de l'information. Ce registre peut contenir, entre autres :
    - La liste des actifs informationnels qui doivent être protégés;
    - La liste des détenteurs d'actifs et leur rôle;
    - La désignation et les attributions du RSIN;
    - Les noms, les titres et les coordonnées de tous les acteurs ou leur substitut en matière de sécurité de l'information ainsi que leurs rôles en la matière et les dates d'entrée en vigueur dans ces fonctions;
- D'assister les détenteurs de l'information pour ce qui est de la catégorisation de l'information relevant de leur responsabilité et de la réalisation des analyses de risques de sécurité de l'information;
- De contribuer à la mise en œuvre des processus officiels de sécurité de l'information de son organisation.

7.6. Responsable de l'accès aux documents et de la protection des renseignements personnels

À titre de responsable délégué par le maire en vertu de la *Loi sur l'accès*, en matière d'accès aux documents et à la protection des renseignements personnels, il coordonne, propose et met en place, les procédures et directives requises pour assurer le respect de la Loi en ces matières. Il conseille les gestionnaires et s'assure que les mesures appropriées sont mises en place dans l'organisation, incluant la formation.

Il veille aussi à l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ., c. A-2.1).

Entre autres :

- Il gère et tient à jour le registre des fichiers de renseignements personnels;
- Il gère le registre des incidents en matière de protection des renseignements personnels;
- Il reçoit, traite et répond aux demandes d'accès à des documents.

7.7. Responsable des archives et de la gestion documentaire (greffier)

À titre de responsable des archives et de la gestion documentaire, le greffier voit à l'établissement et au maintien du calendrier de conservation, du plan de classification et des outils de gestion documentaire de la Ville qui permettent d'assurer la qualité et la conformité du cycle de vie des documents conformément à la Loi sur les archives (RLRQ, c. A-21.1) et les règlements afférents.

7.8. Gestionnaires

- Chaque gestionnaire s'assure que tous les employés sous sa charge connaissent et respectent leurs obligations découlant de la présente politique. Il les informe précisément des normes, des directives et des procédures de sécurité en vigueur;
- Il sensibilise son personnel à l'importance des enjeux de sécurité;
- Il communique au RSIN tout problème d'importance en matière de sécurité de l'information et au responsable de l'accès aux documents et de la protection des renseignements personnels tout incident relatif à la PRP.

7.9. Détenteurs d'actifs informationnels

- Ils s'assurent de la sécurité d'un ou de plusieurs AI qui leur sont confiés en tant que gestionnaire;
- Ils s'impliquent dans l'ensemble des activités relatives à la gestion des risques, notamment l'évaluation, la détermination du niveau de protection visé, l'élaboration des contrôles et la prise en charge des risques résiduels;
- Ils s'assurent que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement;
- Ils déterminent les règles d'accès aux actifs dont ils assument la responsabilité.

7.10. Pilotes de systèmes

- Ils assurent le fonctionnement sécuritaire d'un actif informationnel dès sa mise en exploitation. Il veille à ce que les accès octroyés par les détenteurs aux actifs informationnels dont ils sont responsables soient en place.

7.11. Direction du Service des technologies de l'information

- Elle fournit, implante et maintient en état les moyens techniques et logiques de sécurité et s'assure de leur conformité aux besoins de sécurité déterminés par le détenteur;
- Elle conseille en collaboration avec le RSIN, les détenteurs d'actifs informationnels numériques en matière de protection des actifs informationnels numériques;
- Elle identifie et gère les risques d'atteinte à l'intégrité des actifs informationnels numériques en fonction des exigences des détenteurs d'actifs;
- Elle intègre les orientations et les exigences en matière de sécurité de l'information et de la protection des renseignements personnels lors de la conception, de la réalisation ou de l'entretien de processus d'affaires, des systèmes d'information et des infrastructures technologiques;
- Elle participe à la mise en place et à l'élaboration des solutions de sécurité associées aux demandes de développement de systèmes d'information, en partenariat avec les détenteurs des actifs informationnels et toute personne physique ou morale, qui, par engagement contractuel ou autre, accèdent aux actifs informationnels numériques.
- Elle doit assurer la disponibilité, l'intégrité, la confidentialité, l'accessibilité, l'irrévocabilité de l'information électronique selon les exigences et les droits d'accès définis par le détenteur de l'actif informationnel;
- Elle prend connaissance des événements selon ses champs d'expertise consignés dans le registre des incidents, les analyses et formule des recommandations.

7.12. Direction du Service des ressources humaines

La direction du Service des ressources humaines est responsable d'informer tout nouvel employé de ses obligations découlant de la présente politique.

- Elle veille à la formation et la sensibilisation de l'ensemble du personnel quant 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 en matière de sécurité et de protection de l'information;
- De plus, elle définit le processus disciplinaire des employés relativement aux infractions à la politique de sécurité de l'information;
- Elle doit prendre les mesures nécessaires pour que, lors du départ d'un employé, ses droits d'accès aux AI prennent fin;
- Le changement du statut d'un employé doit ou tout autre événement concernant les tâches et les fonctions de ce dernier doivent conduire systématiquement à la révision et à la suppression, s'il y a lieu, de tous ses accès aux systèmes d'information.

7.13. Comité de sécurité de l'information

Il exerce un rôle-conseil auprès du RSIN. Il évalue les risques et impacts sur la sécurité de l'organisation que les nouveaux projets et les opérations courantes associés aux AI pourraient rencontrer. Il propose des actions quant à la coordination et la mise en œuvre de la politique.

7.14. Utilisateurs

Toute personne visée par la politique, telle qu'elle est définie à la section 3.1, a l'obligation de la respecter afin de protéger l'information mise à sa disposition et de dénoncer tout incident au RSIN en matière de sécurité de l'information et au responsable de l'accès et de la PRP, tout incident en matière de PRP.

8. Dispositions finales

8.1 Sanctions

Le contrevenant à la présente politique ainsi qu'à la réglementation et aux directives qui en découlent s'expose à des mesures administratives, disciplinaires ou légales. Ces mesures doivent être raisonnables, justes et proportionnelles à la gravité et aux impacts des gestes posés.

Ces mesures sont appliquées conformément aux règles et procédures établies dans les lois du travail, les conventions collectives, les ententes établissant les conditions de travail des employés non syndiqués, les contrats individuels de travail, les contrats de service ou dans tout autre document ou texte réglementaire ou législatif applicable.

8.2 Entrée en vigueur

La politique entre en vigueur au moment de son adoption par le conseil de ville.

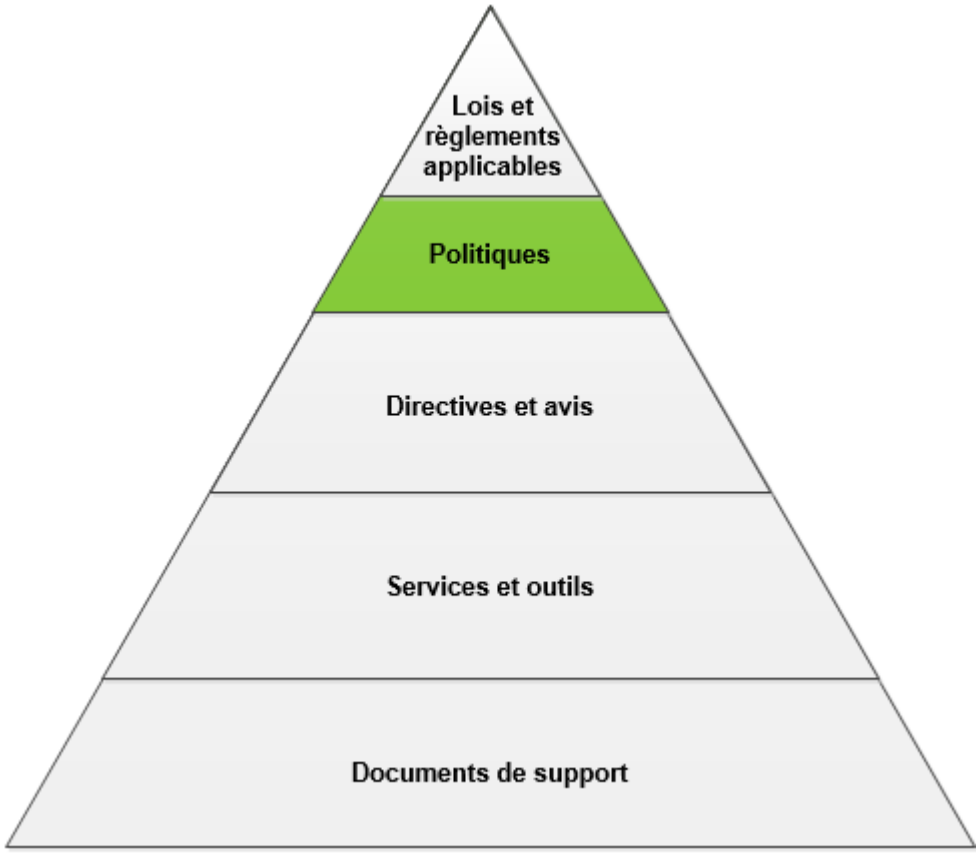
8.3 Mise à jour

La mise à jour de la présente politique relève du RSIN. Elle est révisée chaque année ou à l'occasion d'un changement significatif afin d'assurer son adéquation à l'évolution des besoins, priorités, lois, règlements ou risques ainsi qu'aux changements organisationnels.

Chaque changement significatif sera soumis au conseil de ville pour fins d'acceptation.

ANNEXE I – Cadre normatif Ville de Québec en matière de sécurité de l'information

Le positionnement de la politique [1] s'illustre ainsi :



La politique de sécurité de l'information constitue l'élément clé de notre cadre normatif qui s'appuie sur un cadre légal. Le cadre normatif de sécurité de l'information est constitué d'un ensemble de documents (directives, processus, standards, et autres) qui s'ajoutent et permettent la mise en œuvre de la politique de sécurité de l'information. Ce cadre s'inspire des bonnes pratiques de l'industrie, telles que la série de normes ISO 27000 et du « National Institute of Standards and Technology » (NIST).

[1] **Un cadre de gestion, des directives, des processus et autre document de portée organisationnelle viennent soutenir la mise en œuvre de la politique**

ANNEXE II – DÉFINITIONS

- **Actif informationnel :** Une information, quel que soit son canal de communication (téléphone analogique ou numérique, Internet, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.
- **Catégorisation** : Activité permettant à la Ville d'évaluer le degré de sensibilité de son information, dans le but d'en déterminer le **niveau de protection nécessaire en matière de disponibilité, d'intégrité et de confidentialité (DIC).**
- **Confidentialité :** Propriété d'une information d'être accessible uniquement aux personnes autorisées.
- **Continuité des services :** Capacité d'une organisation d'assurer, en cas de situation d'exception, la poursuite de ses processus d'affaires selon un niveau de service défini par le détenteur responsable de ceux-ci.
- **Cycle de vie de l'information :** Ensemble des étapes que franchit une information et qui vont, du moment où cette information est structurée, jusqu'au moment où elle devient périmée, en passant par les différentes phases (création, enregistrement, transfert, consultation, traitement, transmission, conservation ou sa destruction).
- **Détenteur d'actifs informationnels :** Gestionnaire qui participe à l'ensemble des activités relatives à la sécurité de l'information, notamment l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non informatiques, la prise en charge des risques résiduels concernant les actifs informationnels.
- **Disponibilité** : Propriété d'une information d'être accessible en temps voulu et de la manière requise.
- **Information confidentielle :** Information détenue par la Ville de Québec, peu importe son support, qui n'est pas rendue publique et dont le caractère confidentiel est conféré par une loi.
- **Intégrité** : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation afin d'être considérée exacte et complète lors de son utilisation
- **Mandataire :** Personne pouvant agir au nom d'une autre personne
- **Processus :** Suite d'activités et d'opérations d'une organisation afin de répondre aux besoins de la clientèle et des employés.
- **Renseignement personnel :** Tous les renseignements qui concernent un individu et qui permettent de l'identifier.
- **Ressource informationnelle :** Ensemble des ressources apportant des éléments d'information de différentes natures, qui sont utilisées par une organisation pour mener à bien sa mission. Les ressources informationnelles incluent notamment les ressources humaines, matérielles, financières et technologiques, dans la mesure où elles apportent des éléments d'information.
- **Sécurité de l'information :** Protection résultant de l'ensemble des mesures de sécurité en place pour assurer la disponibilité, l'intégrité et la confidentialité de l'information de la Ville.
- **Technologies de l'information :** Ensemble des matériels, logiciels et services utilisés pour la collecte, le traitement, la conservation et la transmission de l'information.
- **Utilisateur :** Toute personne physique ou morale, groupe ou entité administrative qui fait usage d'un ou de plusieurs AI sous la responsabilité de la Ville de Québec.

ANNEXE III – Principales références documentaires

Les chartes, lois et règlements sont, notamment :

- *Charte canadienne des droits et libertés*, partie I de la Loi constitutionnelle de 1982, [annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R.-U.)];
- *Charte des droits et libertés de la personne du Québec* (R.LRQ., c. C-12);
- *Code civil du Québec* (L.Q., 1991, c. 64), (concernant notamment la protection de la réputation et de la vie privée ainsi que la communication des renseignements confidentiels);
- *Code criminel* (L.R.C., 1985, c. C-46), (concernant notamment l'interception frauduleuse d'informations, la falsification des documents et les méfaits);
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ., c. A-2.1);
- *Loi concernant le cadre juridique des technologies de l'information* (RLRQ., c. C-1.1) (concernant notamment la valeur juridique d'un document technologique et le maintien de l'intégrité durant tout son cycle de vie);
- *Loi sur le droit d'auteur* (L.R.C., 1985, c. C-42);
- Loi sur la sécurité civile, L.R.Q., c. S-2.3;
- Code municipal du Québec, L.R.Q., c. C-27.1 (art. 437.2);
- *Loi sur les archives* (RLRQ., c. A-21.1), (concernant notamment la protection et la conservation des documents ayant une valeur patrimoniale ou archivistique).

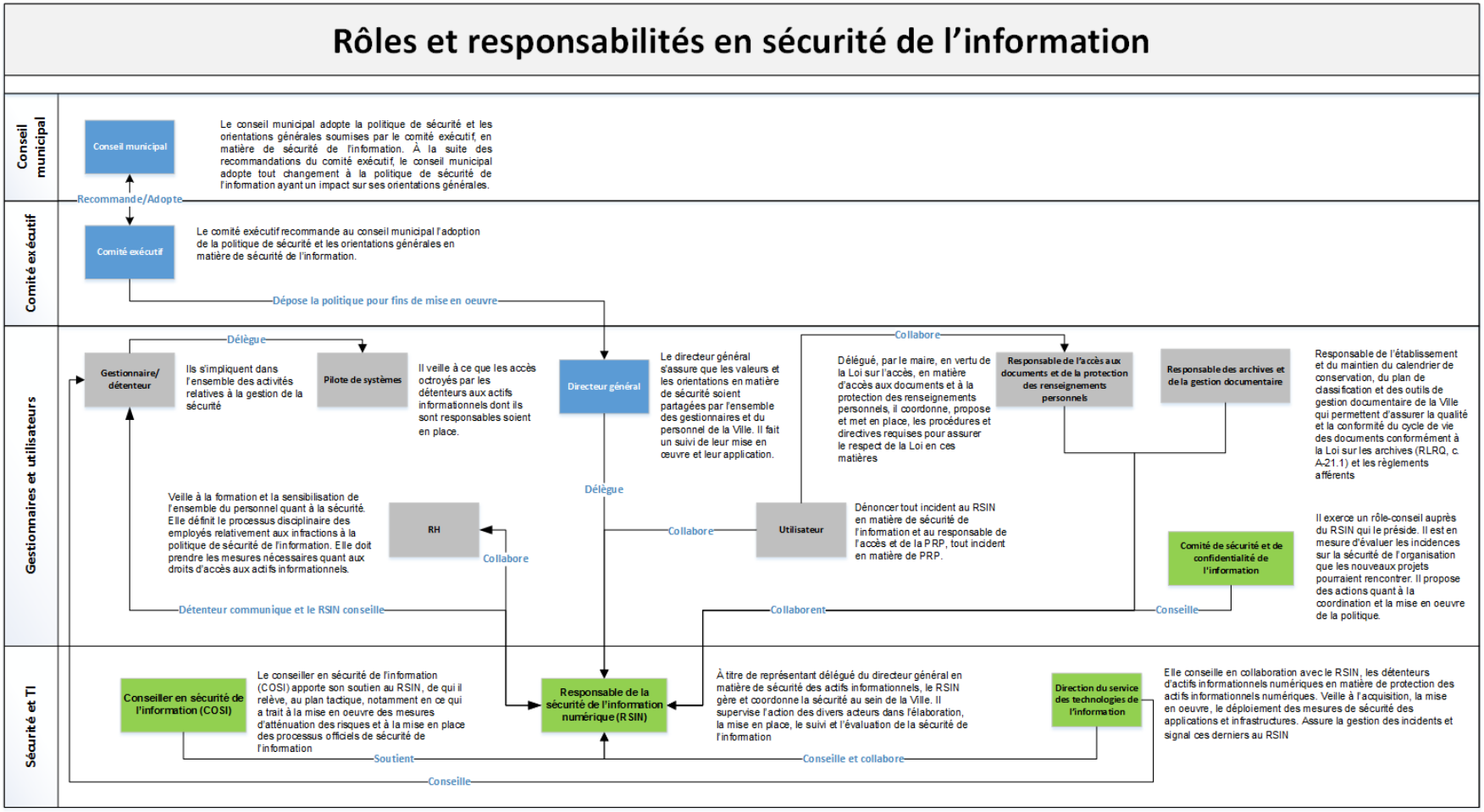
Les lois, chartes et règlements spécifiques à la Ville sont, notamment :

- *Loi sur les cités et villes* (RLRQ., c. C-19);
- *La Loi sur l'éthique et la déontologie en matière municipale (RLRQ*., c. E-15);
- *Charte de la Ville de Québec, capitale nationale du Québec* (RLRQ., c. C-11.5);
- *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (RLRQ c. A21.1 r2);*
- *Règlement sur l'éthique et les règles de conduite des employés de la Ville de Québec* (R.V.Q. 1856).

Références externes et normes

- *Politique de sécurité de l'information de l'organisme – CHU de Québec.*
- *Politique globale de sécurité de l'information de la MRC de Pierre de Saurel*
- *Les normes ISO 27001 et ISO 27002 de l'Organisation internationale de normalisation*
- *La norme du National Institute of Standards and Technology (NIST) 800-53.REV4*

ANNEXE IV – Rôles et responsabilités en sécurité de l'information



Service des technologies de l'information, DGA des services de soutien institutionnels
3 octobre 2018

VILLE DE QUÉBEC l'accent d'Amérique