VILLE DE MASCOUCHE

Politique administrative nº 20170911-01

Objet : **SÉCURITÉ DE L'INFORMATION**

Application : **TOUS LES INTERVENANTS**

Résolution **:**

Date d'entrée en vigueur : 11 septembre 2017

Signatures :

_____*(Signé)*_____
Maire

_____*(Signé)*_____
Greffier

- **LA FORME MASCULINE EST UTILISÉE POUR ALLÉGER LE TEXTE**

Politique numéro 20170911-01

Politique de sécurité de l'information

Service du greffe et des services juridiques
Mars 2017

Paraphes _____ _____ _____

TABLE DES MATIÈRES

I. DISPOSITIONS GÉNÉRALES

1. La sécurité de l'information

L'arrivée des nouvelles technologies a permis d'échanger plus rapidement et plus facilement diverses informations. Cela a aussi entraîné l'apparition de problématiques reliées à la protection des informations confidentielles découlant de ces technologies, telles que les fraudes, le piratage, le vol, la destruction ou la perte de données. C'est dans ce contexte qu'il est important de prendre des mesures appropriées pour assurer la sécurité de l'information.

Dans le cadre de ses activités, la Ville recueille, traite, produit et conserve toutes sortes d'informations sous diverses formes. Ces informations sont essentielles pour le bon fonctionnement de la Ville et ont une valeur légale, économique et administrative. Elles sont présentes à tous les niveaux au sein de l'organisation. À ce titre, la Ville est consciente de l'importance de ces informations et de leur degré de confidentialité. De plus, la Ville est également sensibilisée au fait qu'une mauvaise gestion des informations pourrait ternir l'image et la réputation de la Ville, voire engager sa responsabilité, rendre vulnérable les équipements et infrastructures principales de la Ville, nuire aux opérations administratives ou entraîner des pertes financières pour celle-ci.

De ce fait, afin de respecter ses obligations légales en matière de sécurité de l'information, la Ville désire mettre en place des mesures de protection de l'information et des règles concernant son utilisation.

2. Objectif de la politique

La présente politique constitue une politique de sécurité de l'information visant à réduire les risques auxquels peuvent être exposés les actifs informationnels de la Ville et visant à mettre en place des règles d'utilisation et des mesures de protection appropriées. Le tout, afin d'assurer la protection des renseignements personnels et confidentiels, leur disponibilité et leur intégrité tout au long de leur cycle de vie. Plus précisément, cette politique a pour but de mettre en place des mesures et des mécanismes administratifs et de contrôle afin d'assurer le respect des droits et obligations de la Ville ainsi que des différents intervenants.

Cette politique s'inscrit dans une perspective de sensibilisation et de prévention; elle nécessite l'indispensable collaboration et responsabilisation personnelle et collective de tous les intervenants.

À ce titre, la Ville s'engage à soutenir toutes les actions qui s'inscrivent dans le cadre de cette politique et à mettre de l'avant les moyens nécessaires à leur réalisation afin d'assurer une saine gestion de la sécurité de l'information à la Ville.

Les mesures de sécurité qui seront maintenues ou mises en place devront être proportionnelles à la valeur de l'information à protéger.

Cette politique a également pour but d'assurer un service continu, efficace et efficient à l'information pour les citoyens, le personnel et les autres utilisateurs autorisés, d'assurer la collaboration avec les partenaires, mandataires, consultants et fournisseurs en respectant les ententes contractuelles et enfin, de protéger l'image et la réputation de la Ville comme organisme public responsable.

3. Définition des termes employés et interprétation

Dans la présente politique, et tout autre document s'y rapportant, à moins que le contexte n'impose un sens différent, les mots suivants ou expressions suivantes désignent ou signifient, respectivement :

« **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.

« **Confidentialité** » :

Le caractère réservé d'une information dont l'accès et la diffusion sont limités aux seules personnes autorisées à la connaître.

« **Courriel** » :

Service de correspondance sous forme d'échange de messages électroniques par l'entremise d'un réseau informatique; et tout tel message électronique.

« **Cycle de vie** » :

Ensemble des étapes que franchit une information (électronique ou non) et qui vont du moment où le besoin d'information se fait sentir et où cette information est créée, jusqu'au moment où elle devient périmée et est conservée ou détruite en conformité avec le calendrier de conservation de la Ville, en passant par les différentes phases de son évolution et de sa diffusion.

« **Disponibilité** » :

L'aptitude d'un système à assurer ses fonctions sans interruption, délai ou dégradation au moment même où la sollicitation en est faite.

« **Information** » **:**

Renseignements consignés sur un support quelconque dans un but de transmission des connaissances.

« **Intégrité** » **:**

La protection de l'exactitude et de l'entièreté de l'information et des méthodes de traitement de celle-ci.

« **Intervenant** » :

Tout le personnel (salariés et gestionnaires), membres du conseil municipal, contractuels, sous-traitants, fournisseurs, consultants, mandataires, différents partenaires d'affaires et autres personnes physiques ou morales appelées à avoir accès à l'actif informationnel, aux biens ou aux lieux dont la Ville doit assurer la sécurité.

« **Ville** » :

La Ville de Mascouche.

Les mots ou expressions ci-devant définis ont le même sens qu'ils soient écrits ou non, en tout ou en partie, en caractères gras, en minuscules ou en majuscules.

Dans la présente politique, lorsque le contexte le requiert, le masculin comprend le féminin, et vice-versa, de même que le singulier comprend le pluriel et vice-versa.

Les en-têtes, titres, sous-titres, intitulés, numéros d'articles, de paragraphes et de sous paragraphes de cette politique sont surtout inscrits pour fins de référence et ne doivent pas servir de façon déterminante à son interprétation.

4. Application

4.1. Informations visées

La présente politique est applicable à tout actif informationnel sous la responsabilité de la Ville, et ce, quel que soit son support. Ainsi, toute manipulation, consultation ou utilisation d'information est soumise à la présente politique, tout au long de son cycle de vie.

4.2. Utilisateurs visés

La présente politique est applicable à toute personne physique ou morale ayant accès d'une façon ou d'une autre à l'information sous la responsabilité 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 mandataires,

des consultants, des partenaires, des utilisateurs de services provenant de l'extérieur et des autorités.

5. Principes directeurs

5.1. Gestion du risque

L'élaboration des mesures de sécurité des actifs informationnels devra se faire sur la base de l'identification et l'évaluation périodique des risques menaçant la confidentialité, l'intégrité ou la disponibilité de l'information.

Ces mesures seront déployées selon l'évaluation des impacts et de la probabilité qu'une telle menace survienne et du coût d'implantation de ces mesures; le tout de façon à amoindrir les risques et à les maintenir à un niveau acceptable pour la Ville.

À ce titre, une évaluation des risques devra être effectuée avant toute acquisition ou changement important aux systèmes d'information ou aux infrastructures informationnelles.

5.2. Catégorisation des actifs informationnels

Les actifs informationnels sont assignés à un détenteur, catégorisés et inventoriés.

Ces actifs sont classifiés et protégés selon leur degré de sensibilité et selon les exigences qui sont liées pour assurer leur sécurité.

5.3. Formation et sensibilisation

Le personnel doit être sensibilisé aux menaces et aux conséquences d'une atteinte à la sécurité afin que chacun puisse développer ses réflexes et reconnaître les incidents ou les risques potentiels et ainsi qu'il travaille dans un environnement sécuritaire.

La formation et la sensibilisation à la sécurité informationnelle de manière continue sont essentielles pour assurer la protection des informations.

Le service des ressources humaines et chaque gestionnaire, en collaboration avec le Comité de sécurité de l'information et le responsable de la sécurité de l'information, sensibilisent le personnel à la sécurité des ressources informationnelles.

Tout le personnel a le droit de recevoir les renseignements nécessaires à la bonne compréhension de ces responsabilités en matière de sécurité informationnelle.

Le personnel aura accès à des communications, des documents explicatifs et de la formation.

Le personnel pourra se référer au responsable de la sécurité de l'information pour obtenir des explications ou des renseignements supplémentaires quant aux modalités d'utilisation, de gestion et de protection des actifs informationnels.

5.4. Gestion de l'exploitation et des télécommunications

La Ville s'assure du maintien des infrastructures technologiques et prend les mesures appropriées pour assurer la sécurité des données.

Ces infrastructures sont indispensables au bon fonctionnement de l'organisation; des moyens appropriés sont déployés afin de réduire au maximum les risques de panne et offrir un environnement stable aux intervenants.

Différents mécanismes de surveillance sont prévus afin de détecter les défaillances des systèmes ainsi que tout traitement non autorisé ou malveillant.

5.5. Sécurité physique

La Ville protège physiquement ses ressources informationnelles contre les menaces d'atteinte à la sécurité de l'information et les dangers potentiels pour son environnement : incendie, inondation, survoltage, coupure de courant, accès illégal aux locaux (système d'alarme, serrure, etc.) et autres pannes de diverses natures.

Les mesures sont déployées selon la nature des lieux et des actifs à protéger.

5.6. Contrôle des accès

L'accès aux locaux et aux actifs informationnels doit être contrôlé pour empêcher tout accès non autorisé, tout dommage ou toute intrusion.

Les contrôles d'accès sont mis en place pour permettre ou restreindre l'accès à des zones selon leur degré de sensibilité.

Les accès aux zones déterminées et aux actifs informationnels sont attribués à l'intervenant autorisé en fonction de ce qui lui est nécessaire pour l'exécution de ses tâches, en fonction de son rôle et de ses responsabilités.

Une révision périodique des accès sera effectuée.

Des règles d'utilisation des actifs informationnels sont édictées et des mécanismes de détection d'usage excessif seront mis en place.

5.7. Acquisition, développement et entretien des systèmes d'information

La sécurité doit faire partie intégrante des systèmes d'information afin de protéger la confidentialité et l'intégrité des informations et d'assurer leur disponibilité.

Des règles de sécurité sont établies et suivies tout au long du processus menant à l'acquisition, au développement, à l'implantation et à l'entretien des systèmes d'information.

5.8. Responsabilité des intervenants

La protection de l'information détenue par la Ville s'appuie sur l'engagement continu de l'ensemble des intervenants.

Chaque intervenant a l'obligation de protéger l'information et le matériel mis à sa disposition.

Les intervenants ont des responsabilités spécifiques en matière de sécurité et sont redevables de leurs actions.

Les rôles et responsabilités des intervenants sont clairement définis à tous les niveaux de l'organisation et dans tous les processus d'affaires.

5.9. Gestion du plan de continuité des activités

La Ville doit s'assurer de la continuité des activités nécessaires à la réalisation de ses activités lors d'un sinistre ou d'une défaillance majeure affectant les actifs informationnels jugés essentiels;

Un plan de continuité des affaires, prévoyant notamment une cellule de crise ainsi que des mesures d'urgence est ou sera élaboré afin de limiter les impacts liés à un incident majeur;

L'application de ses mesures facilitera la reprise et la continuité des services essentiels dans les délais établis.

6. Directives afférentes

Pour s'assurer que les lignes directrices régissant la sécurité de l'information soient connues, comprises et appliquées au sein de tous les intervenants, la Ville établira des directives à l'attention de ces derniers, présentant de façon concrète les mesures de sécurité de l'information que ces derniers doivent respecter dans le cadre de leur poste.

7. Gestion des incidents de sécurité de l'information

La Ville mettra en place un processus de gestion des incidents de sécurité de l'information qui vise à traiter rapidement et efficacement tout événement qui cause ou qui pourrait causer un dommage à un intervenant, à un actif informationnel ou tout acte ou omission qui entraîne ou pourrait entraîner la matérialisation d'un risque.

Un intervenant qui contrevient à la présente politique ou à tout autre élément en découlant et qui lui est applicable s'exposera à des mesures administratives, disciplinaires ou légales selon la gravité du contexte et des conséquences de son geste, et ce, conformément aux dispositions de la convention collective ou des ententes s'appliquant.

8. Rôles et responsabilités

8.1. Conseil municipal

Le conseil municipal approuve les orientations générales en matière de sécurité de l'information soumises par le Comité superviseur *ad hoc*;

Suite aux recommandations du Comité superviseur *ad hoc*, il adopte tout changement à la *Politique de sécurité de l'information*.

8.2. Comité superviseur *ad hoc*

- Pour les fins des présentes, l'expression « Comité superviseur *ad hoc* » désigne un comité spécialement formé des membres suivants de la haute direction de la Ville : le maire, le directeur général et le greffier;
- Le Comité superviseur *ad hoc* doit approuver la présente politique, s'assurer de sa mise en œuvre et faire le suivi de son application;
- Il fait les recommandations au Conseil municipal concernant les orientations générales en matière de sécurité de l'information;
- Il fait les recommandations au Conseil municipal concernant l'adoption de tout changement à la politique de sécurité de l'information;
- Il définit les orientations en fonction desquelles les ressources peuvent être affectées et les droits d'accès peuvent être octroyés; il établit les règles d'attribution et de retrait des droits d'accès aux informations, s'assure de leur respect et il autorise toute exception si cela est nécessaire.

8.3. Direction générale

- La Direction générale est la première responsable de la sécurité des actifs informationnels au sein de l'organisation;
- Elle doit s'assurer que les valeurs et les orientations en matière de sécurité sont partagées par l'ensemble des intervenants;
- Elle doit s'assurer de l'application de la *Politique de sécurité de l'information*;
- Elle doit appuyer la mise en œuvre et le développement de ladite politique;
- Elle doit apporter les appuis financiers nécessaires pour la mise en œuvre et l'application de la présente politique, revoir et aligner les investissements et les projets de sécurité de l'information avec les orientations stratégiques;
- Elle doit assurer le respect des rôles et responsabilités des intervenants en regard de leur fonction relativement à la sécurité de l'information; tout en respectant les orientations budgétaires;

8.4. Comité de sécurité de l'information

- Le Comité de sécurité de l'information agit sous l'autorité du Comité superviseur *ad hoc* et de la Direction générale;
- Il doit s'assurer de la réalisation et de la mise en place des différentes politiques, des processus et des directives du cadre de gestion de la sécurité de l'information tant au niveau de l'information elle-même (disponibilité, intégrité, confidentialité), du contrôle des accès, de la sécurité physique des lieux, que des aspects administratifs et légaux assurant la protection de l'information;
- Il valide la *Politique de sécurité de l'information*;
- Il assure la définition, la mise en œuvre, l'organisation et l'évolution du cadre de gestion de la sécurité de l'information en collaboration avec les différentes directions;
- Il élabore et met à jour la politique de sécurité de l'information, la soumet à la Direction générale et au Comité superviseur *ad hoc* pour approbation;
- Il assure le respect général des politiques et procédures de sécurité tant d'un point de vue tactique qu'opérationnel en relation avec les orientations stratégiques;
- Il approuve les critères d'acceptation du risque et les risques résiduels;
- Il propose des plans d'atténuation des risques afin que les détenteurs d'actifs informationnels puissent prendre les bonnes décisions afin de protéger adéquatement ceux-ci;
- Il mesure l'efficacité du système de gestion de la sécurité de l'information et propose des pistes d'amélioration;
- Il recommande les orientations, établit les priorités et tient lieu de forum de coordination et de concertation relativement à la sécurité de l'information;
- Il soutient la Direction générale dans l'exercice de ses responsabilités et l'exécution de ses obligations en matière de sécurité de l'information;
- Il 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;
- Il gère l'implantation de la *Politique de sécurité de l'information*;
- Il définit la méthode d'analyse du risque et les critères d'acceptation du risque;
- Il propose au responsable de la sécurité de l'information, les mesures de contrôle à mettre en place;
- Il crée, au besoin, différents comités et suit l'avancement de leurs travaux;
- En sont membres d'office : la maire, le directeur général, le greffier, le trésorier ou la trésorière, le directeur du Service de l'informatique, le directeur du Service de la sécurité

publique, le Directeur du service de la prévention des incendies et le directeur du Service des travaux publics.

8.5. Responsable de la sécurité de l'information

- Il agit sous l'autorité du Conseil de sécurité de l'information et/ou du greffier;
- 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;
- Il voit à la sensibilisation du personnel 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 (collectés, utilisés, conservés, communiqués ou détruits);
- Il fait approuver par le Comité de sécurité de l'information et le greffier, les documents et activités du plan d'action stratégique en sécurité de l'information et ceux ayant une incidence tactique ou opérationnelle;
- Il 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;
- Il assure la cohérence et la pertinence des interventions en matière de sécurité de l'information;
- Il coordonne et voit à la catégorisation de l'information et des processus d'affaires ainsi que des analyses de risques en matière de sécurité de l'information;
- Il assure le suivi de la politique de sécurité de l'information;
- Il présente au greffier puis 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;
- Il élabore, met en place et maintient à jour le plan de relève des actifs informationnels et des processus d'affaires critiques désignés pas les détenteurs des actifs informationnels;
- Il crée et met à jour le registre d'autorité, le registre des incidents ainsi que la matrice de catégorisation;
- Il traite les non-conformités;
- Il intervient au niveau tactique et opérationnel de l'organisation.

8.6. Gestionnaire

- Il informe son personnel et, le cas échéant, tout intervenant externe, de la présente politique et s'assure de son respect;

- Sujet aux orientations et règles arrêtées par le Comité superviseur *ad hoc*, il 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;
- Il 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;
- Il collabore avec le responsable de la sécurité de l'information aux campagnes de sensibilisation de la sécurité de l'information;
- À titre de détenteur des actifs informationnels affectés aux activités dont il est chargé :
    - il assure une protection adéquate des informations et des processus d'affaires qui lui sont confiés;
    - il gère les attributions ainsi que les retraits des droits d'accès aux informations qui sont sous sa responsabilité et s'assure de leur respect, le tout, en fonction des orientations ou règles établies par le Comité superviseur *ad hoc*;
    - il applique des mesures de contrôle lors de l'utilisation de l'information par les personnes autorisées à y accéder;
    - il catégorise les informations et les processus d'affaires sous sa responsabilité en fonction de la disponibilité, l'intégrité et de la confidentialité;
    - il doit connaître les risques de sécurité de l'information des processus d'affaires sous sa responsabilité;
- Il prend connaissance des événements consignés dans le registre des incidents le concernant, les analyse et formule les recommandations;
- Il prévoit dans les contrats et documents d'appel d'offres le concernant, une clause obligeant tout tiers contractant avec la Ville de respecter les exigences de la *Politique de sécurité de l'information*.

8.7. Salarié

- Il prend connaissance de et se conforme à la politique de la sécurité de l'information; il signe la déclaration solennelle de *Consentement à la Politique de sécurité de l'information* s'y rattachant, en utilisant à cet effet le formulaire figurant à l'Annexe I des présentes; étant bien précisé et entendu que le défaut par un salarié de signer telle déclaration solennelle de *Consentement à la Politique de sécurité de l'information* n'a ni n'aura aucun impact sur son opposabilité à cet intervenant; dans l'éventualité où un salarié a une raison valable d'y déroger, il doit, *via* son gestionnaire, en aviser préalablement le greffier afin d'obtenir une autorisation écrite;
- Il signe, sous forme de déclaration solennelle, un *Engagement à garder la confidentialité*, en utilisant à cet effet le formulaire figurant à l'Annexe II des présentes;
- Il accède à l'information exclusivement dans le cadre de ses fonctions;
- Il limite l'utilisation des actifs informationnels aux fins pour lesquelles ils sont destinés;

- Il 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.

8.8. Intervenant

- Chaque intervenant est responsable d'appliquer et de respecter la présente politique, de même que les normes et les directives en vigueur en matière de sécurité de l'information, nonobstant toute disposition ou stipulation à ce contraire;
- Il doit prendre connaissance de la *Politique de sécurité de l'information* de la Ville;
- Il doit signer la déclaration solennelle de *Consentement à la Politique de sécurité de l'information,* en utilisant à cet effet le formulaire figurant à l'Annexe I des présentes; étant bien précisé et entendu que le défaut par un intervenant de signer telle déclaration solennelle de *Consentement à la Politique de sécurité de l'information*, n'a ni n'aura aucun impact sur son opposabilité à cet intervenant;
- Il doit participer activement à la protection de l'information dans ses activités professionnelles;
- Il doit utiliser les ressources informationnelles en se limitant aux fins pour lesquelles elles sont destinées et à l'intérieur des accès qui lui sont autorisés;
- Il doit respecter le caractère confidentiel des renseignements auxquels il a accès;
- Il doit assurer la sécurité des actifs informationnels de l'organisation au meilleur de ses connaissances et en fonction de ses rôles et responsabilités;
- Il doit aviser le Responsable de la sécurité de l'information de toute situation susceptible de compromettre la sécurité du personnel ou des actifs informationnels;
- Il doit appliquer et respecter l'ensemble des points de la présente politique ainsi que toutes autres politiques, directives, normes ou procédures édictées par la Ville concernant la sécurité de l'information;
- Il doit, selon le cas, soit signer un *Engagement à garder la confidentialité,* sous forme de déclaration solennelle, en utilisant à cet effet le formulaire figurant à l'Annexe II des présentes, soit conclure une entente de confidentialité dont la teneur est conforme à celle du modèle reproduit en Annexe III des présentes ou autrement approuvée par le greffier;
- Il doit signer le consentement à la politique de sécurité de l'information, y adhérer et participer à toute session de formation ou tout programme de sensibilisation mis en place par l'organisation, dans le cas où il fait partie du personnel.

9. Responsabilité des services

9.1. Service du greffe

- Le greffier a la garde des livres, registres, plans, cartes, archives et autres documents et papiers appartenant à la municipalité, ou qui sont produits, déposés et conservés dans le bureau de la

Ville, tel que prévu à la *Loi sur les cités et villes* (RLRQ, c. C-19); le greffier ne peut se dessaisir de la possession d'aucune de ces choses sans la permission du conseil ou l'ordre d'un tribunal;

- Il veille 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);
- Il 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;
- Il coordonne et supervise la mise en œuvre de la Politique de gestion des documents et des archives;
- Il collabore à l'élaboration et à la mise à jour de la matrice de catégorisation et du registre d'autorité;
- Il assure la gestion de l'ensemble des documents administratifs et des archives de la Ville conformément au plan de classification et au calendrier de conservation;
- Il élabore les normes et politiques de gestion, de conservation, de déclassement et de destruction applicables aux documents administratifs et aux archives de la Ville;
- Il prend connaissance des événements concernant ces champs d'expertise consignés dans le registre des incidents, les analyse et formule des recommandations;
- En conséquence, le greffier a un droit de véto et aucune décision ne peut être prise sans son accord, pour tout ce qui peut, directement ou indirectement, avoir un lien avec ou un impact sur tout ce qui est soumis à sa garde de par ou suivant la loi, incluant notamment tout « document » de la Ville au sens donné à ce terme par *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1); aussi, le greffier peut imposer à tout autre intervenant le respect de ses instructions et toute mesure visant à lui garantir le contrôle, assurer la conservation, l'accès, la protection et la sécurité de tout document, toute information ou autre chose placée sous sa garde.

9.2. Service des ressources humaines

- Il 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;
- Il 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;
- Il définit le processus disciplinaire des employés relativement aux infractions à la *Politique de sécurité de l'information*;
- Il s'assure, lors du départ d'un employé, que son droit d'accès aux actifs informationnels prenne fin.

9.3. Service de l'informatique

- Il veille au maintien de la sécurité des technologies supportant l'information numérique;
- Sujet aux orientations et règles arrêtées par le Comité superviseur *ad hoc,* de même qu'aux instructions auxquelles il peut être assujetti en regard de la loi, des présentes ou de la structure hiérarchique organisationnelle, il assure la gestion technique des processus de contrôle d'accès à l'information numérique;
- Il assiste les détenteurs des actifs informationnels dans la mise en place et le maintien d'un environnement sécuritaire d'exploitation des systèmes dont ils sont responsables;
- Il 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;
- Il assure la sécurité des technologies de l'information (techniques et logiques);
- Il assure aux détenteurs 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 détenteurs des actifs informationnels;
- Il 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;
- Il informe et conseille les détenteurs des actifs informationnels et toute autre 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;
- Il identifie et gère les risques d'atteinte à l'intégrité des actifs informationnels numériques;
- Il collabore à l'élaboration et à la mise à jour de la matrice de catégorisation et du registre d'autorité;
- Il prend connaissance des événements concernant ses champs d'expertise consignés dans le registre des incidents, les analyse et formule des recommandations;
- Il surveille les systèmes et les journaux d'activité;
- Il assure la sauvegarde et la récupération des données.

9.4. Services de la sécurité publique, de prévention des incendies et des travaux publics

- Ils identifient 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 veillent à leur mise en place; en tenant compte des orientations et règles arrêtées par le Comité superviseur *ad hoc*, de même que des instructions auxquelles ils peuvent être assujettis ou qui peuvent leur être communiquées en regard de la loi, des présentes ou de la structure hiérarchique organisationnelle;
- Ils procèdent de concert, 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.

II. SANCTIONS EN CAS DE VIOLATION

10. Sanctions applicables

10.1. Sanctions pour le citoyen ou l'utilisateur

En cas de violation des règles de la présente politique ou de toute autre règle établie en conformité avec celle-ci, le citoyen ou l'utilisateur peut se voir retirer immédiatement son droit d'accès et faire l'objet de poursuites judiciaires.

10.2. Sanctions pour le personnel

En cas de contravention à la présente politique ou de toute autres dispositions établies en conformité avec celle-ci, tout membre du personnel, quel que soit sa catégorie d'emploi ou de statut peut être passible de sanctions disciplinaires, administratives ou légales modulées en fonction du principe de la gradation des sanctions, en fonction de la gravité de la contravention, du contexte et des conséquences de la contravention commise par celui-ci. Une contravention à la présente politique par un gestionnaire ou un salarié peut notamment mener à un retrait de son droit d'accès sur le champ, une suspension sans salaire ou à un renvoi et faire l'objet de poursuites judiciaires.

10.3. Sanctions pour les partenaires, mandataires, fournisseurs ou consultants

Tout partenaire, mandataire, fournisseur ou consultant qui contrevient à la présente politique, en outre de toute pénalité pouvant être prévue au contrat les liant à la Ville, peut se voir retirer son droit d'accès immédiatement, se voir résilier unilatéralement son contrat et faire l'objet de poursuites judiciaires.

10.4. Sanctions pour le membre du conseil

Tout membre du conseil qui contrevient à la présente politique peut se voir retirer son droit d'accès immédiatement et faire l'objet de poursuites judiciaires.

III. CADRE JURIDIQUE ET NORMATIF

11. Lois, règlements, directives et normes applicables

La présente politique doit être interprétée en fonction des lois, des règlements, des directives et des normes applicables, 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* (RLRQ, c. 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* (RLRQ, c. A-2.1);
- la *Loi sur les archives* (RLRQ, c. 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'informatio*n (L.R.Q., chapitre C-1.1);
- la *Loi sur les cités et villes* (RLRQ, c. C-19);
- la *Loi sur le droit d'auteur* (L.R.C. chapitre C-42);
- la *Loi sur la fiscalité municipale* (RLRQ, c. F-2.1);
- la *Loi sur les marques de commerce* (L.R.C., 1985, chapitre T-13);
- la *Loi sur la qualité de l'environnement* (RLRQ, c. Q-2);
- la *Loi sur la santé et la sécurité du travail* (RLRQ, chapitre S-2.1);
- la *Loi sur la sécurité civile* (RLRQ, c. S-2.3);
- la *Loi sur la sécurité incendie* (RLRQ, c. 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 (Politique administrative n° XXXX);
- La Politique d'utilisation des outils informatiques de la Ville (Politique administrative n° XXXX);
- la Politique de gestion contractuelle de la Ville (Politique administrative n° XXXX);
- la Politique de gestion des documents et des archives de la Ville (Politique administrative n° XXXX);
- les dispositions de tout code d'éthique adopté par la Ville applicable aux élus et aux employés municipaux.

IV. ENTRÉE EN VIGUEUR

12. Entrée en vigueur de la politique

La présente politique entre en vigueur à compter de son adoption par résolution du Conseil municipal.

ADOPTÉE PAR LE CONSEIL MUNICIPAL LE _____

_____ _____

Maire Greffier

_____

Directeur général

ANNEXE I

CANADA
PROVINCE DE QUÉBEC

DÉCLARATION SOLENNELLE
CONSENTEMENT À LA POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Je, soussigné(e), _____,
déclare solennellement ce qui suit :

1° Je comprends que la VILLE DE MASCOUCHE se soucie de la sécurité de ses actifs informationnels;

2° Je comprends que dans un objectif de sécurité de l'information, la VILLE DE MASCOUCHE a adopté la politique administrative n° 20170911-01, intitulée « *Politique de sécurité de l'information* », dont j'ai pris connaissance, et que cette politique doit s'appliquer à tous les intervenants;

3° Je suis un intervenant au sens de cette politique ou je suis dûment autorisé à représenter l'intervenant dont le nom suit, le cas échéant, étant entendu que dans ce dernier cas j'agis aux présentes tant personnellement qu'au nom de celui-ci et que celui-ci sera autant lié que moi par les présentes, à toutes fins que de droit;

Nom de l'intervenant représenté par le signataire et pour le compte duquel la présente est également faite, le cas échéant : _____;
celui-ci étant par moi dûment représenté à titre de _____;
si je ne suis pas un officier (président, vice-président, etc.), principal dirigeant ou associé de cet intervenant, je joins à la présente les documents démontrant que je suis dûment autorisé à le représenter aux fins des présentes;

4° Je m'engage solennellement, de même que l'intervenant ci-dessus nommé le cas échéant s'engage, sous toutes peines que de droit, à respecter et appliquer la *Politique de sécurité de l'information* (politique administrative n° 20170911-01) de la VILLE DE MASCOUCHE.

Et j'ai signé, à _____,
au Québec, Canada, ce _____.

_____
Signature

DÉCLARÉ SOLENNELLEMENT DEVANT MOI, Me _____,
greffier ou assistante-greffière, ce _____.

_____

ANNEXE II

CANADA
PROVINCE DE QUÉBEC

DÉCLARATION SOLENNELLE
ENGAGEMENT À GARDER LA CONFIDENTIALITÉ

Je, soussigné(e), _____, déclare solennellement ce qui suit :

1° J'ai accepté le poste de _____ pour le service _____ de la Ville de Mascouche;

2° Je comprends que les informations, renseignements, données et documents dont je pourrais prendre connaissance, que l'on pourra me communiquer ou auxquels je pourrais avoir accès dans le cadre de mes fonctions sont et doivent demeurer de nature confidentielle, en toutes circonstances et en tout temps;

3° Je m'engage solennellement et sous toutes peines que de droit à garder confidentiels, ne pas utiliser à des fins personnelles ou au profit de tiers, ni autrement divulguer ou communiquer en tout ou en partie, de quelque façon que ce soit, les informations et données ainsi que les renseignements et documents dont je pourrais prendre connaissance, que l'on pourrais me communiquer ou auxquels je pourrais avoir accès dans le cadre de mes susdites fonctions, pour le service _____ de la Ville de Mascouche, et ce, autant pendant qu'après l'exécution de ces susdites fonctions;

Et j'ai signé, à _____, au Québec, Canada, ce _____.

_____
Signature

DÉCLARÉ SOLENNELLEMENT DEVANT MOI, M^e^ _____, greffier ou assistante-greffière, ce _____.

_____

ANNEXE III

Entente de confidentialité des mandataires et/ou consultants et/ou fournisseurs et/ou partenaires

ENTRE :

VILLE DE MASCOUCHE, personne morale de droit public légalement constituée, ayant son siège social au 3034, chemin Sainte-Marie, à Mascouche, au Québec, Canada, où le code postal est J7K 1P!, ici représentée par _____, _____, et _____, _____, dûment autorisé(e)s à cet effet;

ci-après désignée par le terme « VILLE ;

ET :

_____

_____

_____

_____;

ci-après désigné(e)s par le terme « CONTRACTANT »;

ci-après collectivement appelés "LES PARTIES";

PRÉAMBULE

CONSIDÉRANT QU'en vertu de la *Loi sur les cités et villes* (RLRQ, c. C-19) et de sa politique de gestion contractuelle adoptée par résolution du conseil municipal le _____, la VILLE doit, dans le cadre de l'élaboration, du processus d'attribution et de la gestion des contrats qu'elle octroie ou conclut, garder certaines informations confidentielles;

CONSIDÉRANT QUE le CONTRACTANT peut être soit un mandataire, un consultant, un fournisseur ou un partenaire de la VILLE;

CONSIDÉRANT QU'en date du _____, un contrat de [service ou autre type de contrat] est intervenu entre la VILLE et le CONTRACTANT en vue de ce qui fait l'objet du projet N°_____, incluant notamment ce qui est, le cas échéant, ci-après précisé :

> [*Précision(s) quant à ce qui fait l'objet du contrat préexistant entre la VILLE et le CONTRACTANT* :]
>
> _____
>
> _____
>
> _____
>
> _____;

CONSIDÉRANT QUE, dans le cadre de son contrat exécuté pour le compte de la VILLE, le CONTRACTANT est susceptible d'avoir accès, de prendre connaissance, d'utiliser et de créer divers éléments d'information de nature confidentielle et pour lesquels la VILLE doit en conserver le caractère confidentiel en vertu de la loi;

CONSIDÉRANT QUE la VILLE accepte de divulguer divers éléments d'information de nature confidentielle au CONTRACTANT accepte d'avoir accès, de prendre connaissance, d'utiliser et de créer divers éléments d'information de nature confidentielle, conformément aux modalités prévues dans la présente entente (ci-après appelée "la présente Entente");

CONSIDÉRANT QUE les Parties désirent confirmer leur entente par écrit;

CONSIDÉRANT QUE les Parties ont la capacité et la qualité d'exercer tous les droits requis pour la conclusion et l'exécution de l'entente constatée dans la présente Entente;

EN CONSÉQUENCE DE CE QUI PRÉCÈDE, LES PARTIES CONVIENNENT DE CE QUI SUIT :

1. PRÉAMBULE

Le préambule fait partie intégrante de la présente Entente.

2. OBJET

2.1 Divulgation de l'information confidentielle

Lorsque requis par les exigences découlant du contrat confié, mais toujours à son entière discrétion, la VILLE convient de divulguer au CONTRACTANT divers éléments d'information de nature confidentielle qui appartiennent à la VILLE de façon exclusive ou sont inhérents au contrat confié ou lui sont confiés dans le cadre d'un processus d'appel d'offres (ci-après

collectivement appelés "les éléments d'information confidentielle" ou "l'information confidentielle") conformément aux modalités prévues dans la présente Entente.

2.2 Traitement de l'information confidentielle

Étant susceptible d'avoir accès, de prendre connaissance, d'utiliser et de créer divers éléments d'information confidentielle dans le cadre de son contrat avec la VILLE, le CONTRACTANT convient de traiter cette information confidentielle conformément aux modalités prévues dans la présente Entente.

3. CONSIDÉRATION

3.1 Obligation de confidentialité

Pour bonne et valable considération, dont notamment le maintien de son contrat, le paiement de la rémunération découlant de l'exécution de son contrat ainsi que les autres avantages pouvant découler de ce contrat, le CONTRACTANT s'engage et s'oblige envers la VILLE à :

a) garder secrète et ne pas divulguer l'information confidentielle;

b) prendre et mettre en oeuvre toutes les mesures appropriées pour conserver le caractère secret de l'information confidentielle;

c) ne pas divulguer, communiquer, transmettre, exploiter, utiliser ou autrement faire usage, pour son propre compte ou pour autrui, de l'information confidentielle, en tout ou en partie, autrement que dans le cadre de la présente Entente et pour les fins qui y sont mentionnées; et

d) respecter toutes et chacune des dispositions applicables de la présente Entente.

3.2 Durée de l'obligation de confidentialité

L'obligation de confidentialité du CONTRACTANT demeure en vigueur :

a) pendant toute la durée du contrat confié par la VILLE;

b) pendant une durée illimitée suivant la fin du contrat confié par la VILLE, en ce qui concerne toute information confidentielle relative au mandat confié ou au processus d'appel d'offres ou toute autre information devant être protégée et non divulguée par la VILLE en vertu des lois applicables à cette dernière en cette matière ainsi qu'en vertu de sa *Politique de gestion contractuelle*.

3.3 Remise des éléments d'information confidentielle

À la fin du contrat confié, le CONTRACTANT s'engage et s'oblige envers la VILLE à :

a) remettre à la demande de la VILLE, au Service du greffe de cette dernière ou à tout autre endroit désigné par le greffier, tous les éléments d'information confidentielle en sa possession; et

b) dans ce contexte, ne conserver aucune reproduction (copie, photocopie, brouillon, résumé ou autre), totale ou partielle, sur quel que support que ce soit, de tout ou partie des éléments d'information confidentielle.

3.4 Dénonciation des intérêts pécuniaires ou d'affaires

Le CONTRACTANT affirme ne posséder lui, ses administrateurs et actionnaires aucun lien d'affaires ou intérêts pécuniaires dans les personnes morales, sociétés ou entreprises susceptibles d'être soumissionnaires de la municipalité dans l'appel d'offre relatif au projet n° _____, pour lequel il va agir à titre de mandataire, consultant, fournisseur ou partenaire.

4. SANCTIONS EN CAS DE NON-RESPECT DE LA PRÉSENTE ENTENTE

S'il ne respecte pas l'une ou plusieurs des dispositions de la présente Entente, en tout ou en partie, le CONTRACTANT est passible de l'une ou plusieurs des sanctions suivantes, en plus de celles prévues par la loi et sans préjudice à tout autre droit ou recours de la VILLE :

a) annulation des droits d'accès aux éléments d'information confidentielle concernés par la présente Entente et aux équipements les contenant;

b) résiliation du contrat conclu avec la VILLE;

c) retrait du nom du CONTRACTANT du fichier des fournisseurs de la VILLE;

d) imposition d'une pénalité monétaire équivalente à dix fois (10 X) la valeur du contrat lui ayant été confié par la Ville, exigible à partir du moment où la VILLE a appris le non-respect de la présente Entente, nonobstant tout recours possible en dommages intérêts subis par la municipalité par suite de ce non-respect par le CONTRACTANT.

5. ENTRÉE EN VIGUEUR DE L'ENTENTE

La présente Entente entre en vigueur dès la conclusion du contrat de [*services, entreprise, acquisition ou autre type de contrat*] _____ entre la VILLE et le CONTRACTANT, relativement au projet n°_____.

Dans le cas où cette date est postérieure à la signature de la présente Entente, cette dernière entre en vigueur dès sa signature.

EN FOI DE QUOI, **lecture faite**, les parties ont signé en duplicata, comme suit :

Le **CONTRACTANT**, à _____,
au Québec, le _____,;

[*Nom du contractant* :]

_____

Par :

_____
Nom :_____
Titre :_____

La **VILLE**, à Mascouche, au Québec, le _____
_____;

VILLE DE MASCOUCHE

Par :

_____

_____