Municipalité de Lac-Beauport

Politique régissant la sécurité informatique

Juillet 2022

Résolution : 219-2022

N/Réf.: 192-30-10

Table des matières

1. INTRODUCTION

La sécurité informatique revêt de plus en plus d'importance dans notre société où les échanges accélérés par des moyens technologiques hautement sophistiqués facilitent la diffusion et l'accès de l'information. Or une information plus facilement accessible risque davantage d'être obtenue de manière illicite et utilisée à mauvais escient.

Pour la Municipalité de Lac-Beauport, qui doit collecter de l'information sous toutes ses formes, la conserver et l'utiliser à différentes fins, par exemple pour ses opérations administratives, pour l'exécution et la prestation de ses services ou pour assurer la sécurité de ses citoyens, l'impact d'une manipulation de cette information à des fins illégitimes peut être sérieux. Une telle situation pourrait notamment entraîner des risques financiers, ternir son image et sa réputation, mettre en danger la sécurité des citoyens, engager sa responsabilité, rendre vulnérables les équipements et infrastructures ou nuire aux opérations administratives.

L'information est donc essentielle aux opérations courantes de la Municipalité et, de ce fait, elle doit faire l'objet d'une évaluation, d'une utilisation et d'une protection appropriées.

2. OBJECTIFS DE LA POLITIQUE

Cette politique précise les règles et modalités que les employés doivent respecter en matière d'utilisation des outils informatiques et de communication appartenant à la Municipalité de Lac-Beauport et mis à leur disposition dans le cadre de leur travail. Elle a pour but d'orienter les usagers vers des comportements assurant un environnement informatique structuré, stable et qui assure la protection des données.

Tous les employés qui utilisent les outils informatiques et de communication appartenant à la Municipalité de Lac-Beauport consentent, par leur utilisation, à respecter les règles et modalités établies dans la présente politique.

3. APPLICATION

Cette politique s'adresse à tous les employés municipaux, au conseil municipal ou toute autre personne mandatée pour représenter la Municipalité et ses intérêts.

L'usage des outils informatiques et de communication mis à la disposition de ceux-ci doit se faire dans un contexte professionnel, respectant les lois et règlements en vigueur, la protection de la confidentialité des renseignements et en préservant l'image corporative de la Municipalité de Lac-Beauport. De plus, en utilisant les moyens de communication mis à sa disposition, l'employé doit agir de manière à contribuer au respect d'autrui, au maintien d'un milieu de travail sain, exempt de discrimination, de diffamation ou de harcèlement.

Le responsable de l'application et de la mise à jour de cette politique est le directeur du Service des finances et de l'administration

4. DÉFINITIONS

Outils informatiques et de communication : Pour l'application de la présente politique, le terme outil informatique inclut notamment, mais sans limitation : l'ordinateur, l'ordinateur portable, la tablette, l'accès au réseau Internet, les serveurs, le courrier électronique, le téléphone cellulaire, l'imprimante, le photocopieur, les supports de toutes sortes (disque dur, clé USB, etc.) et logiciels informatiques appartenant à la Municipalité.

Employé : Pour l'application de cette politique, le terme employé inclut tout individu qui exécute un travail, avec ou sans rémunération, pour l'employeur dont les employés permanents, les cadres, les élus municipaux, les employés temporaires et contractuels.

Employeur : La Municipalité de Lac-Beauport.

5. OBLIGATIONS DES UTILISATEURS

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par la Municipalité de Lac-Beauport. À cette fin, il doit :

a) Prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer, en signant la déclaration jointe en annexe 1;

b) Utiliser, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés;

c) Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ou les désactiver;

d) Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;

e) Signaler immédiatement à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la Municipalité;

f) Au moment de son départ de la Municipalité, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition ou produit dans le cadre de l'exercice de ses fonctions.

6. ACCÈS AU RÉSEAU INFORMATIQUE

L'accès au réseau informatique de la Municipalité n'est pas un droit, mais un privilège qui peut être révoqué ou modifié en tout temps.

Pour fins d'identification et de traçabilité, chaque employé devant accéder au réseau informatique reçoit au préalable des codes d'accès uniques. À chacun de ces codes sont associés des droits d'accès spécifiques. Les codes d'usager et mots de passe ne doivent en aucun temps être partagés avec quiconque y compris un autre employé et les postes de travail laissés sans surveillance doivent avoir été verrouillés ou fermés au préalable par l'utilisateur.

7. COURRIER ÉLECTRONIQUE

Les employés se voyant attribuer une adresse de courrier électronique personnelle ont la responsabilité de:

- Consulter régulièrement leur boite de réception et de répondre aux courriels à l'intérieur d'un délai raisonnable;
- Se créer une signature électronique selon les standards établis par le service du greffe;
- Effectuer régulièrement une épuration ou un classement des courriels traités;
- Éviter les courriels trop volumineux;
- Répondre de manière concise et en évitant l'usage de caractères spéciaux, de couleurs ou des lettres majuscules;
- S'assurer que les communications sont empreintes de respect et faites dans un langage courtois;
- Fournir les efforts nécessaires pour éviter les fautes d'orthographe autant pour les communications internes qu'externes;
- Utiliser la fonction « répondre à tous » ou « cc » lorsque plusieurs intervenants sont concernés;
- Utiliser le gestionnaire d'absence pour informer les expéditeurs d'une absence du travail et de la date de retour prévue.

À chacun des départements est associé une adresse de courriel générique permettant de centraliser les communications générales. Chacune de ces boîtes de courriels se doit d'être gérée quotidiennement par les employés désignés.

8. SAUVEGARDE DES DONNÉES

Les données stockées sur les serveurs de la Municipalité font l'objet d'une sauvegarde quotidienne dans des lieux physiques distincts de la salle informatique centrale. Cette pratique permet de sécuriser l'intégrité des informations et ces copies peuvent servir à récupérer des données accidentellement perdues.

Puisqu'aucune sauvegarde n'est effectuée sur les postes de travail individuels (disque local C:), tous les documents, y compris les documents de travail ou d'ébauches, doivent être enregistrés uniquement sur les serveurs informatiques en respectant le plan de classification. Il est de la responsabilité de chacun des usagers de respecter ce système et de classer ses documents dans les bons répertoires, et ce, au fur et à mesure. Les nouveaux fichiers doivent comporter un titre court et qui décrit bien le contenu. Selon le cas, l'ajout d'une date au titre permet également de mieux les classer dans les différents dossiers.
La personne responsable de la documentation peut aider les employés à classer correctement les différents documents. Se référer à la *politique de gestion des documents* de la Municipalité qui établit les fondations de la gestion documentaire en incluant la gestion numérique des documents.

9. USAGE D'INTERNET

La Municipalité met à la disposition des employés un accès à Internet pour réaliser les tâches reliées à leur fonction. Il est cependant, et non limitativement interdit de :

- Utiliser Internet à des fins personnelles durant les heures travail sur quelque support que ce soit (ordinateur, portable, tablette, cellulaire, etc.) ;
- Utiliser Internet pour consulter du matériel obscène, à caractère violent ou sexuel;
- Consulter tout type de contenu inapproprié et hors contexte du milieu de travail;
- Utiliser des applications superflues qui auraient pour effet de surcharger inutilement les systèmes informatiques (par exemple écouter la radio ou des vidéos sur Internet);

Des mécanismes de filtrage sont mis en place par l'employeur afin de limiter l'accès à certains sites et un contrôle aléatoire et/ou ciblé peut être effectué en cas de doute du non-respect de cette règle.

10. RÈGLE D'UTILISATIONS DES OUTILS INFORMATIQUES ET DE COMMUNICATION

Sans être limitatifs, sont des usages interdits des outils informatiques et de communication :

1. Utiliser le matériel de communication de la Municipalité afin de tenir des propos offensants, diffamatoires et harcelants envers qui que ce soit;

2. Partager des codes d'usagers et des mots de passe;

3. Exécuter tout travail ou activité commerciale qui n'est pas relié à ses fonctions;

4. Consulter des sites Internet ou utiliser des applications qui ne sont pas reliés à ses fonctions;

5. Accéder illégalement à des informations confidentielles ou en faire la distribution;

6. Introduire intentionnellement des troubles ou des virus informatiques;

7. Télécharger ou installer des logiciels ou progiciels non autorisés par l'employeur;

8. Participer à des activités de piratage informatique;

9. Usurper l'identité d'un individu lors de l'utilisation des outils informatiques et de communication de la Municipalité;

10. Intercepter, surveiller ou enregistrer une communication dont il n'est pas partie prenante;

11. Consulter, s'approprier ou transmettre des informations violant les lois de propriété intellectuelle et d'accès à l'information;

12. Créer, télécharger et distribuer des informations à caractère sexuel explicite, jeux, vidéo, logiciels ou fichiers verbalement ou visuellement contre les bonnes mœurs;

13. Participer à des groupes de discussions qui n'ont pas de lien avec le travail ;

14. S'approprier des documents internes pour un usage autre que professionnel de même que tout acte volontaire visant à détruire ou à compromettre l'intégrité des données.

11. INTELLIGENCE ARTIFICIELLE (IA)

L'intelligence artificielle, terme générique, décrit une vaste gamme de méthodes, de technologies, d'algorithmes, dont la finalité est d'automatiser des tâches qui habituellement pourraient être conduites par des humains.

La Municipalité permet aux employés l'usage de logiciels d'IA à condition que :

- Les logiciels utilisés sont uniquement ceux fournis et payés par l'employeur;
- L'usage de ceux-ci est effectué dans un contexte professionnel, respectant les lois et règlements en vigueur, la protection de la confidentialité des renseignements et en préservant l'image corporative de la Municipalité de Lac-Beauport;
- L'employé se conforme à toutes les règles d'utilisation des outils informatiques et de communication du paragraphe 10.

12. SÉCURITÉ

La sécurité des systèmes informatiques est à prendre au sérieux et doit faire partie des priorités. Depuis les dernières années, de plus en plus nombreuses sont les institutions victimes de cyberattaques et les conséquences qui en résultent sont très importantes (perte de données, pertes financières, mises à pied d'employés, etc.).

La direction de la Municipalité s'assure que le réseau informatique est protégé contre les intrusions ou les attaques malveillantes par l'installation et la mise à jour d'un système de pare-feu et d'antivirus.

Les usagers doivent adopter les comportements suivants :

- Ne jamais relier d'outils informatiques personnels au réseau de la Municipalité;
- Ne jamais cliquer sur des communications qui semblent suspectes (courriels, liens, etc.), la vigilance est requise en tout temps;
- En cas de doute sur une intrusion d'un virus ou d'une cyberattaque, avertir immédiatement le responsable informatique ou votre supérieur immédiat.

13. VIE PRIVÉE

L'employé qui utilise les outils informatiques et de communication de la Municipalité acquiesce que les informations échangées ou sauvegardées au moyen de ceux-ci deviennent accessibles en tout temps par l'employeur. L'utilisation de ces outils se fait en sa qualité d'employé.

14. TÉLÉTRAVAIL

Le télétravail se définit comme étant le fait qu'un membre du personnel exécute ses tâches, sur une base régulière ou non, à distance, à l'extérieur des bureaux, par le biais de différents moyens technologiques fournis par l'employeur.

En situation de télétravail, l'employé consent, par l'utilisation des outils informatiques et de communication de la Municipalité, à respecter les mêmes règles et modalités qu'établies dans la présente politique de même que la *politique de télétravail*.

15. SANCTIONS

Lorsqu'un utilisateur contrevient à la présente politique ou aux directives en découlant, il s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conditions de travail.

ANNEXE

Déclaration d'engagement par les utilisateurs quant au respect des règles de sécurité informatique

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition par la Municipalité. À cette fin, ils doivent :

1- Se conformer à la politique régissant la sécurité informatique de la Municipalité;

2- Utiliser, dans le cadre des droits d'accès qui leur sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les actifs informationnels mis à leur disposition, en se limitant aux fins auxquelles ils sont destinés;

3- Respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier la configuration des mesures de sécurité ou les désactiver;

4- Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;

5- Signaler immédiatement à leur supérieur tout acte dont ils ont connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la Municipalité;

6- Au moment de leur départ de la Municipalité, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie qui avaient été mis à leur disposition dans le cadre de l'exercice de leurs fonctions;

7- Je soussigné(e), _____, reconnais avoir pris connaissance des règles, ci-dessus reproduites, de la politique régissant la sécurité informatique de la Municipalité et m'engage à les respecter.

Signature : _____ Date : _____