VILLE DE SAINT-JEAN-SUR-RICHELIEU

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Service des Technologies de l'Information

Politique : POL-CORP-007

Adoptée par le CM : 18 juin 2024

NO RÉSOLUTION – CM-20240618-6.1

TABLE DES MATIÈRES

1. PRÉAMBULE

Dans le contexte d'un niveau de menaces de plus en plus sophistiquées et de leurs impacts en hausse, la Ville de Saint-Jean-sur-Richelieu (la Ville) reconnaît l'importance de la sécurité de l'information pour protéger ses données, ses infrastructures, ainsi que d'assurer la confiance de ses citoyens en la matière.

À cette fin, la Ville met en œuvre un programme conçu pour identifier, évaluer et mitiger les risques liés à la sécurité de l'information de manière à être alignée à ses besoins, ses risques et ses objectifs. Ce programme englobe l'ensemble des ressources, projets et initiatives en sécurité de l'information ainsi qu'un cadre de gestion comportant un ensemble de politiques, de directives, de procédures, de contrôles et d'une architecture de sécurité inspirés de normes et référentiels reconnus dans le domaine.

Dans le cadre de ce programme, pour orienter ses actions et pour démontrer ses intentions, la Ville s'est dotée de cette politique qui émet les principes fondamentaux, les obligations générales et les rôles et responsabilités des parties prenantes à la Ville en matière de confidentialité, intégrité et disponibilité de ses services.

2. PRINCIPES

Le programme de sécurité de l'information comporte cinq (5) principes qui guideront sa conception, sa mise en œuvre et son opération :

Gouvernance et transparence
Les décisions du programme sont alignées avec la stratégie, les objectifs, les besoins, les exigences réglementaires et les risques de la Ville avec une reddition de comptes pour la performance de celui-ci.

Gestion du risque
Un standard de gestion des risques basé sur la norme ISO27005 pour identifier, évaluer, mitiger et suivre les risques et la posture de risque en sécurité de l'information en continu.

Protection des données
Le cadre de gestion en sécurité de l'information soutient la gouvernance des données de la Ville en alignant ses contrôles de protection pour respecter la réglementation sur la protection des renseignements personnels.

Cyber-résilience
Une architecture de sécurité encadre les contrôles de protection, de détection et de résilience contre les cybermenaces, incluant aussi des plans de continuité des affaires et de reprise des opérations documentés et à jour.

Sensibilisation et formation
La Ville met en œuvre un programme de sensibilisation et de formation pour éduquer et outiller ses usagers sur les menaces et réagir aux incidents de cybersécurité ainsi que leur rôle dans la protection des données.

3. OBJECTIFS

La présente politique a pour objectifs :

3.1 D'affirmer clairement les principes et les attentes de la Ville en termes de sécurité de l'information pour toutes ses parties prenantes;

3.2 De baliser les obligations que toutes ces parties doivent respecter en continue lorsqu'elles utilisent ses actifs informationnels;

3.3 D'identifier les rôles et les responsabilités de chaque entité à la Ville en lien avec la politique et le programme de sécurité de l'information.

4. CHAMPS D'APPLICATION

La politique s'applique aux élus, à tous les employé(e)s de la Ville, réguliers, à temps plein ou à temps partiel, temporaires et contractuels, syndiqués ou non syndiqués, y compris les cadres de tout niveau.

5. CADRE RÉGLEMENTAIRE

Le programme de sécurité de l'information soutient la conformité de la Ville aux lois et règlements auxquels la Ville est soumise. Les lois applicables sont, notamment, les suivantes :

- ✓ Loi sur les cités et villes
- ✓ Loi sur l'organisation territoriale municipale
- ✓ Loi sur les compétences municipales
- ✓ Loi sur les élections et les référendums dans les municipalités
- ✓ Loi sur la fiscalité municipale
- ✓ Loi sur le traitement des élus municipaux
- ✓ Loi sur l'éthique et la déontologie en matière municipale
- ✓ Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
- ✓ Loi sur les dettes et les emprunts municipaux
- ✓ Loi concernant les droits sur les mutations immobilières
- ✓ Loi sur les travaux municipaux
- ✓ Loi sur l'interdiction de subventions municipales
- ✓ Loi sur les immeubles industriels municipaux
- ✓ Loi sur la sécurité civile
- ✓ Loi sur l'aménagement et l'urbanisme
- ✓ Loi sur la qualité de l'environnement
- ✓ Loi sur l'expropriation

6. OBLIGATIONS GÉNÉRALES

Les obligations générales suivantes identifient les attentes de chaque utilisateur des actifs informationnels de la Ville.

6.1. Protection des actifs informationnels

a) Les actifs informationnels sont attribués à un propriétaire et catégorisés selon leur niveau de criticité et ils sont inventoriés par le service des technologies de l'information dans un inventaire centralisé et normalisé.

b) Seuls les dispositifs autorisés par la Ville peuvent avoir accès à ses actifs informationnels.

c) Les obligations d'utilisation des actifs informationnels sont détaillées dans les directives internes d'utilisation acceptable de ceux-ci.

d) Il est interdit de bloquer la mise à jour automatique ou automatisée, de désactiver ou contourner les contrôles de sécurité tels que l'antivirus, le chiffrement ou le contrôle centralisé des actifs informationnels de la Ville.

e) Seuls les logiciels approuvés par le service des technologies de l'information peuvent être installés sur ses actifs informationnels.

f) Avant d'introduire ou d'installer un nouveau logiciel ou nouvel outil, le Service des technologies de l'information (TI) doit être impliqué.

g) Avant de contracter ou de faire l'utilisation d'un nouveau service infonuagique, le Service des approvisionnements et le Service des technologies de l'information doivent être impliqués.

6.2. Sécurité des données

a) La protection de l'information détenue par la Ville s'appuie sur l'engagement continu de l'ensemble des intervenants. Chacun a l'obligation de protéger les données à sa disposition.

b) Les obligations en termes de la protection et de la gestion des renseignements personnels sont définies dans la **politique-cadre sur la gouvernance (protection des renseignements personnels)**.

c) Les propriétaires des actifs informationnels et des données doivent se conformer aux contrôles de gestion d'accès et ne fournir l'accès qu'aux utilisateurs le nécessitant.

d) Les utilisateurs ne doivent accéder qu'aux données et systèmes nécessaires et approuvés pour leur rôle.

e) Les données doivent être protégées lors du stockage et de la transmission par des protocoles de chiffrement approuvés.

f) Le traitement des données doit suivre le cycle de gestion des documents et archives tel que défini dans la **politique de gestion des documents et des archives**.

6.3. Gestion de l'identité et contrôle d'accès

a) Les identifiants doivent être uniques pour chaque utilisateur, avec des mots de passe forts, uniques et changés selon les exigences de la Ville.

b) Les usagers ne doivent pas partager leur identifiant ni le noter de manière non-sécurisée.

c) Un mécanisme d'authentification multifactorielle est exigé pour certaines application et plateformes et il est interdit de partager ce deuxième facteur avec un autre usager ou contourner son implémentation ou son intention.

d) Les accès aux actifs informationnels doivent être revus à intervalles réguliers. L'examen doit inclure la suppression dans les plus brefs délais des accès qui ne sont plus nécessaires.

6.4. Sensibilisation et formation

a) Les utilisateurs doivent assister à des formations périodiques sur la sensibilisation à la sécurité de l'information et les diverses activités du programme telles que mises à disposition par la Ville et requises selon leur rôle et responsabilités.

6.5. Gestion des incidents de sécurité de l'information

a) Les utilisateurs doivent être vigilants face aux comportements ou alertes inattendues et ont l'obligation de signaler ces événements au Service des technologies de l'information.

b) Lorsque requis, les utilisateurs doivent se familiariser avec les plans de réponse aux incidents ou de continuité des affaires de la Ville définis, et signaler tout changement de responsabilité qui pourrait impacter certaines étapes de réponse aux incidents.

c) Les utilisateurs, dans le cadre d'une réponse à un incident de sécurité de l'information, doivent supporter l'équipe de gestion des incidents dans leurs actions d'analyse ou de mitigation en fournissant les informations nécessaires sur les anomalies observées et suivre les instructions de celle-ci.

d) Après un incident, les utilisateurs doivent soutenir les efforts de retour à la normale en suivant les instructions de l'équipe de gestion des incidents de sécurité de l'information.

e) Les utilisateurs nécessaires aux activités et plans après un incident, doivent participer et exécuter ceux-ci.

6.6. Gestion des changements

a) Tous les changements impliquant des actifs informationnels doivent suivre le processus de gestion des changements, à savoir la planification, l'évaluation, la révision, l'approbation et la documentation, afin de minimiser l'impact négatif sur les services informatiques, les utilisateurs et nos citoyens.

6.7. Gestion du risque

a) Le choix des mesures de protection des actifs informationnels s'appuie sur une évaluation périodique des risques et a pour objet d'atténuer et maintenir le niveau de risque acceptable pour la Ville.

b) Les utilisateurs ayant des actions assignées dans les plans de mitigations approuvés par la direction doivent exécuter leurs tâches et faire le suivi du plan.

c) Des tests d'intrusion ou des balayages de vulnérabilité sur tout actif informationnel ont lieu périodiquement ou selon les exigences des lois et règlements applicables, et sont coordonnés par la sécurité de l'information afin de déterminer les risques et/ou les vulnérabilités potentielles.

7. RÔLES ET RESPONSABILITÉS

Les responsabilités des différentes parties prenantes de la Ville dans la mise en place et l'opération de cette politique et du programme de sécurité de l'information.

7.1. Conseil Municipal

a) Adopte la politique de sécurité de l'information et ses modifications.

b) Approuve les orientations générales soumises par la Direction Générale en matière de sécurité de l'information.

c) S'assure du respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ainsi que toutes autres lois applicables.

7.2. Direction Générale

a) Présente la politique de sécurité de l'information et ses modifications ainsi que les orientations générales au conseil municipal.

b) Supporte la politique de sécurité de l'information au moyen de directives claires, d'un engagement, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.

d) S'assure de la mise en application des exigences de la politique et du programme dans les services sous-jacents.

7.3. Direction des services

a) S'assure du respect de la politique de sécurité de l'information par les utilisateurs de leur service en leur diffusant et en les sensibilisant à ses exigences.

b) À tire de propriétaire d'actifs informationnels, elle s'assure de la protection adéquate des informations et des processus d'affaires qui lui sont confiés ainsi que leurs plans de continuité.

c) Collabore avec l'officier de sécurité de l'information dans la mise en œuvre et le respect des exigences du programme de sécurité de l'information.

7.4. Officier de sécurité de l'information

a) Recommande les orientations, établit les priorités et tient lieu de forum de coordination et de concertation relativement à la sécurité de l'information.

b) Soutient la Direction générale dans l'exercice de ses responsabilités en matière de sécurité de l'information et assure la surveillance ainsi que l'application de cette politique de sécurité.

c) Sensibilise de manière continue les utilisateurs quant à la sécurité des actifs informationnels.

d) Effectue une vigie des menaces, vulnérabilités et tendances pour aligner stratégiquement et en continu le programme de sécurité de l'information et intégrer les mitigations des risques émergents.

e) Établit les exigences et approuve l'architecture de sécurité et y documente les responsabilités et les outils nécessaires à celle-ci.

f) Met en place et tiens à jour un plan de réponse aux incidents de sécurité et tiens un rôle clé dans la prise en charge de ceux-ci.

g) Surveille la performance des contrôles de sécurité, identifie les écarts et pistes d'amélioration, et prépare des tableaux de bord pour les comités et parties prenantes nécessitant une reddition de comptes du programme.

7.5. Propriétaires d'actifs informationnels

a) Opèrent les actifs informationnels dont ils sont propriétaires de manière conforme.

b) Approuvent la stratégie de gestion des accès à ses actifs informationnels pour qu'elle soit conforme au niveau de sécurité de ceux-ci.

c) Répondent au cycle de revues des accès de la Ville.

d) Mitigent les risques et exécutent les plans d'actions approuvés par la direction générale.

e) Notifient le Service des technologies de l'information dès la découverte de tout événement pouvant entraîner un incident de sécurité ou de confidentialité.

7.6. Coordonnateur municipal des mesures d'urgence

a) Quantifie et qualifie le risque en matière de sécurité de l'information dans la matrice de risques majeurs à la Ville.

b) Gère et coordonne les incidents en sécurité de l'information de sévérité 1.

c) Supporte l'officier de sécurité de l'information pour la gestion et la coordination des incidents de sévérité 2.

7.7. Service des technologies de l'information

a) Met en œuvre une architecture de sécurité répondant aux besoins de la Ville ainsi qu'aux exigences du cadre de gestion.

b) Met en œuvre des outils pour la surveillance de cette architecture et des infrastructures informationnelles de la Ville.

c) Opère les outils de surveillance et répond aux alertes et aux événements détectés par ceux-ci.

d) S'assure des opérations de l'infrastructure de sécurité de l'information et des plans de retour après sinistre ou incident.

7.8. Utilisateurs d'actifs informationnels

a) Respectent la présente Politique de sécurité de l'information et l'ensemble des mesures implantées en fonction de celle-ci.

b) Utilisent les actifs informationnels uniquement dans le cadre de leurs fonctions et aux fins auxquels ils sont destinés.

c) Signalent promptement à leur supérieur immédiat, leur contact à la Ville ou au Service des technologies de l'information tout événement, anomalie ou risque à la sécurité ou à la confidentialité de l'information.

8. MANQUEMENTS ET SANCTIONS

Tout manquement, par un(e) employé(e), à une règle prévue à la présente politique ou à une directive qui en découle peut entraîner, sur décision de la Ville et dans le respect de tout contrat de travail, l'application de toute sanction appropriée à la nature et à la gravité du manquement, pouvant même aller jusqu'au congédiement.

9. RÉVISIONS ET MODIFICATIONS

Cette politique doit être révisée aux deux ans à des fins d'alignement aux besoins de la Ville, de son cadre réglementaire, des changements à son environnement organisationnel ainsi que des risques et menaces émergeantes. Elle peut être revue hors cycle pour des raisons exceptionnelles.

Toutes révisions et tous changements doivent être approuvés au Comité Exécutif.

ANNEXE – DÉFINITIONS

Actif informationnel : Toute donnée, application, système informatique ou tout autre élément qui contient ou traite de l'information et qui est d'importance pour les opérations de la Ville. Les actifs informationnels sont soumis à des politiques de classification et de gestion du risque pour assurer leur confidentialité, leur intégrité et leur disponibilité.

Confidentialité : Caractère des données dont l'accès et la diffusion doivent être limités, par des mesures de protection des données, aux seules personnes ou autres entités autorisées.

Disponibilité : Propriété d'un système informatique ou d'une donnée capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

Incident de confidentialité : Désigne toute consultation, utilisation ou communication non autorisées par la loi d'un Renseignement personnel, ou toute perte ou autre atteinte à la protection de ce renseignement.

Incident de sécurité de l'information ou de cybersécurité : Tout événement imprévu ou indésirable qui pose un risque pour la sécurité aux actifs informationnels. Cela peut inclure des événements causant un déni d'un ou plusieurs services, une perte de données ou un accès non-autorisé à un actif informationnel ou au réseau.

Intégrité : Propriété des données qui ne subissent aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.

Menace : Événement potentiel et appréhendé, susceptible de porter atteinte à un système informatique.

Politique de Sécurité : Énoncé général émanant de la direction d'une organisation, et indiquant la ligne de conduite adoptée relativement à la sécurité informatique, à sa mise en œuvre et à sa gestion.

Programme de Sécurité de l'Information : Ensemble des activités, processus, politiques, directives, technologies servant à assurer et aligner la posture de risque en sécurité de l'informations à celle de l'organisation. Le programme inclus aussi l'architecture et le cadre de gestion de sécurité ainsi que les outils nécessaires à gouvernance du domaine.

Renseignement personnel : Désigne toute information qui concerne une personne physique et qui permet de l'identifier directement — soit par le recours à cette seule information — ou indirectement — soit par combinaison avec d'autres informations.

Risque : Probabilité plus ou moins grande de voir une menace informatique se transformer en événement réel entraînant une perte.

Vulnérabilité : Faiblesse d'un système informatique se traduisant par une incapacité partielle de celui-ci à faire face aux attaques ou aux intrusions informatiques.