MUNICIPALITÉ DE
Saint-Ferréol
les-Neiges

POLITIQUE DES MESURES DE SÉCURITÉ DES PROCESSUS INFORMATIQUES

Adopté le 11 août 2025

Résolution numéro 25-249

Table des matières

1. Objet, champ d'application et utilisateurs

Le présent document a pour objet d'assurer le fonctionnement ordonné et sécurisé des technologies de l'information de la municipalité de Saint-Ferréol-les-Neiges (la « **Municipalité** »).

Les utilisateurs de ce document sont les employés et les sous-traitants de l'unité d'affaires des technologies de l'information de la Municipalité

2. Référence documents

- Politique cadre de protection des renseignements personnels
- Politique de gestion intégrée des documents et de sécurité de l'information
- Politique de protection des données sur le lieu de travail

3. Procédures de sécurité

3.1 Gestion du changement

Chaque modification des systèmes opérationnels ou de production doit être effectuée de la manière suivante :

1. le changement peut être proposé par tout employé utilisant le système sujet à modification. Dans ce contexte la personne sera nommée le porteur de la demande;
2. le changement doit être autorisé par le directeur général, qui doit évaluer la raison du changement pour la Municipalité et les impacts positifs et négatifs potentiels sur la sécurité;
3. les changements doivent être mis en œuvre par la compagnie responsable d'offrir le service de support ou par le fournisseur de services gérés;
4. Le directeur général est chargé de vérifier que le changement a été mis en œuvre conformément aux requis présentés dans la présente politique;
5. Le porteur de la demande est responsable des tests et de la vérification de la stabilité du système – le système ne doit pas être mis en production avant que des tests approfondis aient été effectués;
6. la mise en œuvre des changements doit être signalée à tous les employés via une nouvelle intranet;
7. La formation requise doit être données aux employés touchés par le changement.

Les enregistrements de modification sont conservés au sein du registre des systèmes réseaux, d'exploitation et de production de la Municipalité.

4. Sauvegarde

4.1 Procédure de sauvegarde

Des copies de sauvegarde doivent être créées pour tous les systèmes de la Municipalité selon la fréquence adéquate.

Le responsable des TI est responsable de s'assurer de la sauvegarde des informations, des logiciels et des images système.

Des audits du processus de sauvegarde doivent être effectués selon le calendrier prévu.

4.2 Test des copies de sauvegarde

Les copies de sauvegarde et le processus de leur restauration doivent être testés au moins une fois par année en implémentant le processus de restauration des données sur le serveur prévu à cet effet en vérifiant que toutes les données ont été récupérées avec succès.

Le responsable des TI est responsable du test des copies de sauvegarde. Les dossiers sur les copies de sauvegarde d'essai sont conservés au sein du registre des tests des copies de sauvegarde.

5. Gestion de la sécurité réseau

Le responsable des TI, à travers le contrat de services gérés, est responsable de la gestion et du contrôle des réseaux informatiques, de la sécurité de l'information dans les réseaux et de la protection des services connectés aux réseaux contre les accès non autorisés. Il est donc nécessaire :

1. de séparer la responsabilité opérationnelle des réseaux de la responsabilité des applications sensibles et d'autres systèmes;
2. de protéger les données sensibles transitant sur le réseau public;
3. de protéger les données sensibles qui transitent sur les réseaux sans fil;
4. de protéger l'équipement qui se connecte au réseau à partir d'emplacements;
5. de séparer le trafic provenant d'appareils mobiles, configurer des stratégies de pare-feu uniques, des itinéraires statiques, des réseaux locaux virtuels, etc.;
6. d'assurer la disponibilité des services;
7. de mettre en place des contrôles de routage pour s'assurer des contrôles d'accès;
8. le responsable des TI doit selon le calendrier des audits s'assurer de la surveillance et du test des contrôles mis en œuvre.

6. Services réseau

Le responsable des TI doit définir les caractéristiques de sécurité et le niveau de services attendus pour tous les services de réseau, que ces services soient fournis en interne ou externalisés – ces exigences doivent être documentées avec les fournisseurs de services.

Si les services réseau sont externalisés, les exigences doivent être spécifiées dans l'accord avec le fournisseur de services.

7. Surveillance du système

Sur la base des résultats de l'évaluation des risques et sous recommandation du fournisseur de services gérés, le responsable des TI décide quels journaux seront conservés sur quels systèmes et pour quels systèmes, et pour combien de temps ils seront stockés. Les journaux doivent être conservés pour tous les administrateurs et opérateurs de système dans un endroit à accès restreint.

Le responsable des TI est imputable de s'assurer de la surveillance quotidienne des journaux relatifs aux défauts signalés automatiquement, ainsi que de l'enregistrement des défauts signalés par les utilisateurs, afin d'analyser les raisons pour lesquelles des erreurs se sont produites et de prendre les mesures correctives appropriées. Des autorisations spécifiques peuvent être spécifiées pour les actions en cas d'erreur, ainsi que la façon dont les enregistrements des erreurs sont conservés.

Le fournisseur de services gérés est chargé d'examiner régulièrement les journaux afin de surveiller les activités des utilisateurs, des administrateurs et des opérateurs de système. L'examen est effectué à des intervalles prescrits par le responsable TI, qui détermine et sélectionne les dossiers à examiner, et comment l'examen mis en œuvre sera enregistré. Le directeur général doit être informé des résultats de l'examen.

8. Gestion des registres tenus sur la base de ce document

Nom du registre	Emplacement de stockage	Personne responsable de l'entreposage	Contrôle de la protection des enregistrements	Période de rétention
Registre des systèmes réseaux, d'exploitation et de production	04-201	Responsable TI	Une fois créé, l'enregistrement ne peut pas être modifié ultérieurement	3 ans
Registre des journaux de sauvegarde	Services gérés	Services gérés	Services gérés	Les documents sont conservés pendant une période de 1 an
Registre des SLA	04-202	Responsable TI	Seul les cadres ont le droit d'accéder à ces dossiers	5 ans après l'expiration de l'accord ou du service fourni
Registre des journaux de pistes d'audit des systèmes informatiques	04-204 Sécurité et risque informatique	Responsable TI	Seul les cadres ont le droit d'accéder à ces dossiers. Les journaux sont en lecture seule ; ils ne peuvent être supprimés ou modifiés	Les journaux sont conservés pendant une période de 5 ans

9. Validité et gestion des documents

Ce document est valide à partir du 12 août 2025.

Le propriétaire de ce document est la municipalité de Saint-Ferréol-les-Neiges, et son Responsable de la protection des renseignements confidentiels doit vérifier et, si nécessaire, mettre à jour le document au moins une fois par an à moins qu'une situation particulière justifie la révision de façon plus rapide.

_____

Mélanie Royer-Couture, mairesse

_____

Eric Ennis, directeur général et trésorier