RÈGLEMENT NUMÉRO 249-16

RÈGLEMENT ÉDICTANT LA POLITIQUE GLOBALE DE SÉCURITÉ DE L'INFORMATION DE LA MRC DE PIERRE-DE SAUREL

ATTENDU que la MRC consacre d'importantes ressources à l'acquisition, au développement et à l'entretien des équipements et des technologies permettant la saisie, la conservation, l'échange et la diffusion de l'information;

ATTENDU que depuis l'implantation de son réseau de fibre optique, la MRC partage ce réseau avec la majorité des municipalités qu'elle regroupe;

ATTENDU que la MRC met également à la disposition de ces municipalités un service de soutien informatique;

ATTENDU qu'il y a lieu d'encadrer par une politique globale de sécurité de l'information le partage de ce réseau, que ce soit pour accéder à des documents internes ou pour accéder à Internet;

ATTENDU qu'un avis de motion a été dûment donné à la séance ordinaire du 14 octobre 2015, le tout conformément aux dispositions de l'article 445 du *Code municipal du Québec* (L.R.Q., c. C-27.1);

ATTENDU qu'une copie du projet de ce règlement a été remise aux membres du Conseil au moins deux jours juridiques avant la tenue de la présente séance;

ATTENDU que des copies de ce projet de règlement sont à la disposition du public pour consultation depuis le début de la séance;

ATTENDU que les membres du Conseil déclarent avoir lu ce projet de règlement et renoncent à sa lecture par la greffière;

ATTENDU que l'objet du règlement et sa portée ont été mentionnés par la greffière;

EN CONSÉQUENCE, il est proposé par M. le Conseiller régional Jean-François Villiard, appuyé par M. le Conseiller régional Luc Cloutier et résolu à l'unanimité que le Conseil de la MRC de Pierre- De Saurel adopte le présent règlement numéro 249-16 et décide, par ce règlement, ce qui suit :

ARTICLE 1 – PRÉAMBULE

Le préambule du présent règlement en fait partie intégrante.

ARTICLE 2 - OBJET

Le présent règlement a pour objet d'édicter la Politique globale de sécurité de l'information de la MRC de Pierre-De Saurel, le tout afin d'assurer le respect de toute obligation opérationnelle et de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information et des télécommunications.

ARTICLE 3 – POLITIQUE GLOBALE DE SÉCURITÉ DE L'INFORMATION

La Politique globale de sécurité de l'information de la MRC de Pierre-De Saurel jointe à l'annexe A est adoptée dans son entier et fait partie intégrante du présent règlement comme si elle était ici au long reproduite.

ARTICLE 4 – ENTRÉE EN VIGUEUR

Le présent règlement entrera en vigueur conformément à la loi.

Serge Péloquin, préfet suppléant	M^{e} Jacinthe Vallée, greffière

ADOPTÉ À L'UNANIMITÉ à la séance ordinaire du Conseil de la MRC du 20 janvier 2016.

Annexe A – Politique globale de sécurité de l'information

Avis de motion :	14 octobre 2015
Adoption :	20 janvier 2016
Entrée en vigueur :	19 février 2016

POLITIQUE GLOBALE DE SÉCURITÉ DE L'INFORMATION DE LA MRC DE PIERRE-DE SAUREL

ANNEXE A – Règlement numéro 249-16

Table des matières

1. INTRODUCTION

La Municipalité régionale de comté (MRC) de Pierre-De Saurel est une entité administrative, regroupant douze municipalités, qui assure la gestion de services régionaux et joue un rôle essentiel dans la réalisation de projets visant l'amélioration de la qualité de vie des citoyens, et ce, dans une perspective de développement durable.

En vertu de certaines lois, la MRC doit assurer la gestion de certains dossiers tels que :

- l'aménagement du territoire;
- la gestion des cours d'eau;
- la gestion des matières résiduelles;
- la sécurité publique, incendie et civile;
- l'évaluation foncière;
- la vente des immeubles pour défaut de paiement de taxes foncières.

La MRC assure également, de façon facultative, la gestion de certains dossiers comme :

- la protection des boisés;
- le développement local et régional sur son territoire;
- le transport collectif;
- le Parc éolien Pierre-De Saurel;
- les équipements à caractère supralocal;
- le réseau informatique;
- le service de soutien informatique offert aux municipalités et aux organismes utilisant le Réseau informatique.

Depuis l'implantation de son réseau de fibre optique, la MRC partage ce Réseau avec la majorité des municipalités qu'elle regroupe (incluant, mais sans s'y limiter, les bureaux municipaux, les bibliothèques et autres locaux). La MRC met également à la disposition de ces municipalités un service de soutien informatique. Non seulement l'utilisation interne du Réseau informatique de la MRC doit être encadrée par une politique globale de sécurité de l'information, mais le partage de ce Réseau, que ce soit pour accéder à des documents internes ou pour accéder à Internet, présente des enjeux au niveau de la sécurité informatique.

La MRC consacre d'importantes ressources à l'acquisition, au développement et à l'entretien des équipements et des technologies permettant la saisie, la conservation, l'échange et la diffusion de l'information. La Disponibilité, l'accessibilité et la portée illimitée des équipements et de leur utilisation requièrent l'établissement de Procédures et de règles d'utilisation et de conduite, répondant ainsi au besoin de protéger les actifs de l'organisme, de protéger les droits des Utilisateurs du Réseau informatique et de prévenir l'organisme des menaces actuelles et futures que représente l'utilisation partagée du Réseau informatique de la MRC.

1.1. DÉFINITIONS

Dans cette politique, à moins que le contexte ne s'y oppose, les expressions suivantes signifient ce qui suit :

« Actif informationnel » : Information numérique, Banque d'informations numériques, système ou support d'information, documentation, Technologie de l'information, installation ou ensemble de ces éléments, reliés ou non au Réseau informatique, acquis ou constitués par une organisation;

« Administration » : Fonction permettant de gérer les processus et les outils de sécurité entourant les équipements, les Logiciels et les Réseaux;

« Application » : Ensemble organisé de moyens informatiques (traitements, données et interfaces), incluant les progiciels, mis en place pour recueillir, traiter, emmagasiner, communiquer et éliminer l'information dans le but de répondre à un besoin déterminé et de soutenir les processus de travail des Utilisateurs;

« Authentification » : Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif;

« Banque d'informations » : Ensemble d'informations relatives à un domaine défini, regroupé et organisé de façon à en permettre l'accès;

« Confidentialité » : Propriété d'une information devant être accessible qu'aux personnes autorisées;

« Continuité» : Propriété qu'a la Ressource informationnelle d'être accessible de la manière requise (sans interruption, délai ou dégradation) et utilisable au moment voulu;

« Contrôle d'accès » : Fonction permettant aux systèmes de contrôler l'accès aux ressources selon des autorisations préalablement accordées aux Utilisateurs;

« Cycle de vie de l'information numérique » : Période de temps couvrant toutes les étapes d'existence de l'information numérique dont celles de la définition, de la création, de l'enregistrement, du traitement, de la diffusion, de la conservation et de la destruction de cette information;

« Détenteur » : Gestionnaire à qui est assignée la responsabilité de la sécurité d'un Actif informationnel et/ou d'un processus d'affaires;

« Disponibilité » : Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée;

« Fournisseur » : Organisme privé ou public ou personne physique faisant affaire avec un Utilisateur en vue de lui fournir des services ou des biens informatiques;

« Intégrité » : Propriété d'une information ou d'une Technologie de l'information de n'être ni modifiée, ni détruite sans autorisation;

« Irrévocabilité » : Propriété d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré;

« Logiciel » : Ensemble de programmes et procédés relatifs au traitement informatique des données;

« Procédure » : Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche;

« Renseignement confidentiel » : Renseignement qui ne doit pas être divulgué à des personnes non autorisées comme l'indiquent des dispositions de la Loi sur l'accès aux documents des organismes publics et la protection des Renseignements personnels;

« Renseignement personnel ou nominatif » : Renseignement qui concerne une personne physique et qui permet de l'identifier;

« Réseau » : Ensemble d'équipements qui sont reliés les uns aux autres par des câbles, des faisceaux hertziens ou Wi-Fi afin qu'ils puissent échanger, distribuer ou diffuser des informations et partager différentes ressources. Une connexion par câble de fibre optique constitue une extension inhérente du Réseau local de la MRC. Par ce fait, tout organisme connecté au Réseau de la MRC par le biais d'un câble de fibre optique est considéré comme faisant partie du Réseau local de la MRC;

« Ressource informationnelle » : Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs;

« Risque » : Menaces, impacts et vulnérabilités auxquels l'information et les infrastructures de traitement de l'information sont exposées;

« Surveillance » : Fonction permettant de détecter les vulnérabilités et les intrusions affectant les Réseaux, les serveurs, les Applications et les informations;

« Technologie de l'information » : Tout Logiciel, matériel électronique ou combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, reproduire, protéger ou éliminer de l'information numérique;

« Utilisateur » : Toute personne de la MRC, de quelque catégorie d'emploi que ce soit ayant accès à l'Actif informationnel, ainsi que toute personne morale ou physique

qui, par engagement contractuel ou autrement, accède à l'Actif informationnel de l'organisme. Cela peut comprendre, mais sans s'y limiter, les municipalités et les organismes municipaux, les Fournisseurs et les consultants.

1.2. OBJECTIFS

La présente politique vise à assurer le respect de toute obligation opérationnelle et de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information et des télécommunications en informant les Utilisateurs des actifs informationnels de la MRC de leurs rôles et de leurs responsabilités.

Plus spécifiquement, les objectifs de la MRC en matière de sécurité de l'information sont :

- d'identifier, de réduire et de contrôler les Risques pouvant porter atteinte aux informations ou aux systèmes d'information de la MRC, des municipalités et des organismes municipaux;

- d'assurer l'Intégrité, l'Irrévocabilité, la Disponibilité, la Confidentialité, l'Authentification, le Contrôle d'accès, la Surveillance et l'Administration à l'égard de l'utilisation des Réseaux informatiques, des télécommunications et d'Internet, de l'utilisation des actifs informationnels et des données administratives;

- d'assurer le respect de la vie privée des individus, notamment la Confidentialité des Renseignements à caractère nominatif relatifs aux Utilisateurs et au personnel de la MRC et à ceux des municipalités et des organismes municipaux;

- d'assurer la conformité aux lois et règlements applicables ainsi que les directives, normes et orientations gouvernementales;

Cette politique sera suivie de règlements et de Procédures afin de préciser les obligations qui en découlent.

1.3. RESPECT DE LA POLITIQUE

Le directeur général de la MRC, nommé par le Conseil de la MRC, est le responsable de la présente politique et est chargé de son application.

La MRC exige de toute personne qui utilise ses actifs informationnels, ou qui y a accès par l'entremise de son Réseau, de se conformer aux dispositions de la présente politique ainsi qu'aux Procédures et aux règlements qui s'y rattachent.

1.3.1. Mesures de contrôle

La MRC se réserve le droit de prendre des mesures raisonnables et appropriées dans le but de superviser et de contrôler l'utilisation faite des équipements informatiques et des Réseaux mis à la disposition des Utilisateurs et de déterminer si ces équipements et ces Réseaux sont utilisés conformément à la présente politique.

La MRC peut notamment procéder à des contrôles, périodiques ou ponctuels, par des moyens électroniques ou autres, de tout équipement informatique, de tout matériel électronique, de tout fichier, de toute information téléchargée, des sites Internet visités et, dans certaines circonstances, du courrier électronique, utilisant ou connecté aux actifs informationnels de la MRC.

1.4. CHAMP D'APPLICATION

La présente politique en matière de sécurité de l'information ainsi que les règlements et les Procédures qui lui sont associés, notamment le Règlement sur l'utilisation et la gestion des actifs informationnels de la MRC, s'appliquent aux personnes, aux activités de même qu'aux actifs énumérés ci-après.

1.4.1. Personnes visées

Tous les Utilisateurs ayant accès, authentifié ou non, à l'Actif informationnel de la MRC, que ce soit au moyen du Réseau (filaire ou Wi-Fi), de supports de stockage (clés USB, disques durs externes, etc.) ou par tout autre moyen, et ce, avant, durant et après leur mandat, leur contrat ou tout autre type de collaboration avec la MRC.

Cela comprend, mais sans s'y limiter, les gestionnaires et les employés de la MRC, les municipalités et les organismes municipaux desservis par le Réseau de la MRC, les abonnés des bibliothèques de ces municipalités, les Fournisseurs et les consultants utilisant et ayant accès à l'Actif informationnel de la MRC ou ayant des actifs de la MRC sous leur garde.

1.4.2. Actifs visés

Cette politique s'applique aux trois catégories d'actifs informationnels suivants :

- ceux appartenant à la MRC et exploités par cette dernière;
- ceux appartenant à la MRC et exploités ou détenus par un Fournisseur de services, par un consultant, par une municipalité ou par un organisme municipal;

- ceux appartenant à un Fournisseur de services ou à un tiers et exploités par lui au profit de la MRC.

1.4.3. Activités visées

Toutes les activités impliquant la manipulation ou l'utilisation sous toutes ses formes des actifs informationnels de la MRC sont visées par la présente politique, que celles-ci soient conduites dans ses locaux ou dans un autre lieu, comme défini dans le Règlement sur l'utilisation et la gestion des actifs informationnels de la MRC.

2. CADRE JURIDIQUE ET NORMATIF

La présente politique a été conçue et doit être appliquée et interprétée en fonction des lois générales (voir annexe 1), des règlements, des directives, des normes et des standards énumérés ci-après.

2.1. DIRECTIVES ET RÈGLEMENTS

- Le Code d'éthique et de déontologie des employés de la MRC de Pierre-De Saurel;

- Le Règlement sur l'utilisation et la gestion des actifs informationnels de la MRC de Pierre-De Saurel;

La MRC ne peut, en vertu de la présente politique ou autrement, forcer un Utilisateur à contrevenir à un autre code d'éthique ou de déontologie adopté en vertu d'une loi.

2.2. NORMES ET STANDARDS

- La norme ISO/IEC 27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information;

- L'architecture gouvernementale de la sécurité de l'information numérique (AGSIN);

- Le modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise.

3. PRINCIPES DIRECTEURS

3.1. GÉNÉRALITÉS

Cette politique globale de sécurité de l'information est fondée sur les énoncés généraux suivants :

- tous les Utilisateurs ayant accès aux actifs informationnels de la MRC assument des responsabilités spécifiques en matière de sécurité et sont redevables de leurs actions auprès du responsable de la présente politique;

- la mise en œuvre et la gestion de la sécurité reposent sur une approche globale et intégrée des aspects humains, organisationnels, financiers, juridiques et techniques, et demandent, à cet égard, la mise en place d'un ensemble de mesures coordonnées;

- les mesures de protection, de prévention, de détection, d'assurance et de correction doivent permettre d'assurer la Confidentialité, l'Intégrité, la Disponibilité, l'Authentification et l'Irrévocabilité des actifs informationnels de même que la Continuité de la Ressource informationnelle. Elles doivent notamment empêcher les accidents, l'erreur, la malveillance ou la destruction d'information sans autorisation;

- les mesures de protection des actifs informationnels doivent permettre de respecter les lois existantes en matière d'accès, de diffusion et de transmission d'informations de même que les obligations contractuelles de la MRC, des municipalités et des organismes municipaux;

- une évaluation périodique des Risques et des mesures de protection des actifs informationnels doit être effectuée afin d'obtenir l'assurance qu'il y a adéquation entre les Risques, les menaces et les mesures de protection déployées;

- la gestion de la sécurité de l'information doit être incluse et appliquée tout au long du processus menant à l'acquisition, au développement, à l'utilisation, au remplacement ou à la destruction, par ou pour la MRC, d'un Actif informationnel appartenant à la MRC et/ou aux municipalités et aux organismes municipaux;

- les éléments de sécurité relatifs à la gestion des postes de travail, des comptes et des accès pour les Utilisateurs, des serveurs informatiques, de la sauvegarde et la récupération des informations, des processus d'exploitation, des Applications et de l'accès au Réseau de la MRC doivent faire l'objet d'un règlement plus précis.

3.2. PROTECTION DES ACTIFS INFORMATIONNELS

Plus spécifiquement, cette politique globale de sécurité de l'information est fondée sur les obligations suivantes en matière de protection des actifs informationnels :

3.2.1. Classification

Les actifs informationnels doivent faire l'objet d'une identification et d'une classification. Le niveau de protection de chaque Actif informationnel doit être identifié par son Détenteur en fonction de sa criticité, de sa sensibilité et des Risques d'accidents, d'erreurs et de malveillance auxquels il est exposé.

3.2.2. Protection des locaux et du matériel

- Tous les accès physiques à des locaux comportant des actifs informationnels appartenant à la MRC doivent être contrôlés afin d'empêcher tout dommage ou toute intrusion. Des équipements appropriés de Contrôle d'accès doivent être mis en place à l'entrée de ces locaux en fonction des Risques identifiés;

- Tout support d'information appartenant à la MRC et devant être déplacé hors des locaux sécurisés doit faire l'objet d'une Surveillance continue et de mesures de contrôle appropriées selon son degré de criticité afin de le préserver de tout dommage;

- Personne ne doit détruire sans autorisation le matériel appartenant à la MRC. Tout dommage doit être rapporté et expliqué au Détenteur de l'actif concerné. On ne peut disposer d'un actif sans avoir d'abord prévu une méthode de recyclage ou de mise aux rebuts sécurisée.

3.2.3. Utilisation des informations et des installations reliées

- Les droits et les privilèges doivent être alloués selon le profil d'utilisation;

- Les actifs informationnels doivent être protégés et utilisés avec discernement et aux seules fins prévues, soit la sécurité, l'intégralité de l'information et les traitements effectués sur les équipements;

- Personne ne doit modifier ou détruire, sans autorisation de la part du service de soutien informatique, les actifs de la MRC;

- Seules les personnes dûment autorisées par le service de soutien informatique peuvent utiliser les actifs de la MRC;

- L'utilisation des actifs informationnels de la MRC est un privilège et non un droit. Ce privilège peut être révoqué, en tout temps, pour tout Utilisateur qui ne se conforme pas à la présente politique et aux règlements s'y rattachant. Les actifs informationnels comprennent, mais sans s'y limiter, le Réseau de la MRC (filaire et Wi-Fi) et le matériel informatique.

3.2.4. Postes de travail

- Tout usage prohibé d'un poste de travail connecté au Réseau de la MRC, comme défini dans le Règlement sur l'utilisation et la gestion des actifs informationnels, peut entraîner des sanctions;

- Tous les postes de travail connectés au Réseau de la MRC doivent comporter des mesures de protection approuvées par la MRC contre les accès non autorisés et les vulnérabilités logicielles;

- Tous les accès et privilèges doivent être régis par des règles d'identification et d'Authentification ainsi que par des profils d'utilisation selon les responsabilités et les fonctions de chaque Utilisateur;

- Tout Utilisateur du Réseau de la MRC doit être informé de ses responsabilités vis-à-vis des informations que lui confie l'organisme et sensibilisé aux moyens de protection disponibles.

3.2.5. Systèmes d'information institutionnels, serveurs et Réseaux locaux

- Tout système d'information doit être protégé, au minimum, par un processus d'accès nécessitant un mécanisme d'identification et d'Authentification de l'Utilisateur. Il doit, en plus, limiter cet accès aux personnes autorisées seulement, en fonction de la nature de l'information et des Applications utilisées;

- Chaque Utilisateur doit obtenir un compte unique permettant de retracer son parcours au travers des systèmes d'information de la MRC. Tous les comptes des Utilisateurs doivent nécessiter un mot de passe. Seuls des mots de passe et identifiants sécuritaires doivent être utilisés;

- Le départ, le transfert, la mutation ou tout autre événement concernant les tâches et les fonctions d'un Utilisateur doivent conduire systématiquement à la révision et à la suppression, s'il y a lieu, de tous ses accès au système d'information;

- Toute information sise sur un serveur doit faire l'objet d'une sauvegarde appropriée selon son degré de criticité. De plus, l'archivage de ces informations doit être conforme aux règles internes et légales établies;

- Un plan de Continuité et de relève des services informatiques de la MRC doit être mis en place et faire l'objet de tests de simulation périodiques en tout ou en partie.

3.2.6. Protection des Applications et des processus d'exploitation

- Le principe du « droit d'accès minimal » doit être appliqué en tout temps lors de l'attribution d'accès aux actifs informationnels. Des droits d'accès limités doivent être attribués à l'Utilisateur autorisé en fonction de ce qui lui est strictement nécessaire pour l'exécution de ses tâches;

- 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;

- L'environnement servant à effectuer la maintenance des Applications et des processus reliés doit être isolé de l'environnement réel de production;

- L'acquisition, le développement et la maintenance des Applications doivent être règlementés et contrôlés par le service de soutien informatique pour éviter la possibilité d'insertion, intentionnelle ou non, de codes malveillants;

- Les Applications ou les processus d'exploitation susceptibles d'occasionner des répercussions sur l'information critique de la MRC, des municipalités et des organismes municipaux ne doivent être accessibles que par l'intermédiaire de moyens sécurisés dans un environnement contrôlé et restreint;

- Toute Application (la documentation reliée, les Logiciels utilisés et les processus nécessaires à son exécution) doit faire l'objet d'une sauvegarde appropriée pour répondre aux critères de Disponibilité, d'Intégrité et de Confidentialité déterminés par son Détenteur d'actifs;

- Toute opération critique effectuée sur ou par l'intermédiaire d'une Application ou d'un processus d'exploitation doit pouvoir être retracée par le service de soutien informatique à l'aide de journaux d'événements correctement sécurisés et préservés pour références futures;

- Les ententes et les contrats dont la MRC, les municipalités et les organismes municipaux font partie pour 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 MRC.

3.2.7. Protection des Renseignements confidentiels et stratégiques

- Toute information considérée confidentielle ou stratégique doit être protégée contre tout accès ou toute utilisation non autorisé ou illicite;

- Sont notamment jugés confidentiels au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des Renseignements personnels, les Renseignements nominatifs, les renseignements relatifs à la vie privée de la personne au sens du Code civil du Québec ainsi que tout renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne;

- L'attribution à un Utilisateur d'un accès à des données confidentielles doit être précédée d'un engagement formel de cet Utilisateur au respect des règles élémentaires de protection des moyens d'accès fournis et du devoir de signalement en cas de divulgation non autorisée (ou même de suspicion de divulgation d'information stratégique);

- Les Renseignements personnels doivent être utilisés et servir qu'aux fins pour lesquelles ils ont été recueillis ou obtenus;

- L'Utilisateur ne peut transmettre de Renseignements personnels sans le consentement des personnes concernées à l'exception des cas prévus par la Loi sur l'accès aux documents des organismes publics et sur la protection des Renseignements personnels;

- Tout produit informationnel issu de systèmes informatisés ou de télécommunication de la MRC et contenant de l'information confidentielle doit être conservé de façon sécuritaire et détruit ou mis aux rebuts selon les standards de sécurité, de Confidentialité et éventuellement d'archivage, lorsque sa détention ou son utilisation n'est plus nécessaire.

3.2.8. Courrier électronique

Dans le but de lutter contre la propagation et l'exécution de codes malveillants, l'interception d'informations sensibles, la désinformation (ou le pollupostage) et la publication d'informations illégales, diffamatoires ou de harcèlement, la MRC établit les règles suivantes quant à l'utilisation du courrier électronique.

Pour tout message électronique diffusé sur le Réseau de la MRC, l'Utilisateur :

- doit s'identifier à titre de signataire de son message et préciser, s'il y a lieu, à quel titre il s'exprime;

- doit respecter la Confidentialité des messages transportés sur le Réseau et s'abstenir d'intercepter, de lire, de modifier ou de supprimer tout message qui ne lui est pas destiné;

- doit utiliser des moyens sécurisés sur le poste dont il se sert pour transmettre des données sensibles vers ou depuis l'extérieur de la MRC;

- doit éviter de surcharger le système de messagerie;

- ne doit d'aucune façon utiliser, sans autorisation, un ou des subterfuges ou d'autres moyens pour transmettre un courrier électronique de façon anonyme ou en utilisant le nom d'une autre personne;

- ne doit capter, stocker, reproduire ou transmettre (au moyen du Réseau de télécommunication vers une boîte vocale ou une adresse électronique) du matériel ou un message à caractère illégal;

- ne doit se servir de l'adresse de courriel ou de la messagerie électronique à des fins commerciales ou illicites, ou en faciliter l'utilisation à ces fins;

- ne doit en aucune façon expédier, sans autorisation, à tous les employés de la MRC, des municipalités et des organismes municipaux, des messages sur des sujets d'intérêt divers, des messages à des fins commerciales, des nouvelles de toutes sortes, des lettres en chaîne et toute information non pertinente aux activités de la MRC;

- ne doit pas répondre à un courrier électronique de provenance douteuse et/ou 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.

3.3. SIGNALEMENT DES INCIDENTS

Tout Utilisateur a l'obligation de signaler sans tarder au gestionnaire ainsi qu'au directeur général adjoint de la MRC, ou, en son absence, le directeur général, de tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité comme le vol, l'intrusion dans un Réseau ou un système, des dommages délibérés, l'utilisation abusive, la fraude, etc.

3.4. DROITS DE PROPRIÉTÉ INTELLECTUELLE

Les Utilisateurs des actifs informationnels de la MRC doivent se conformer aux exigences légales sur l'utilisation de produits à l'égard desquels il pourrait y avoir

des droits de propriété intellectuelle et sur l'utilisation de produits Logiciels propriétaires, comme défini dans le Règlement sur l'utilisation et la gestion des actifs informationnels de la MRC.

3.5. CONTINUITÉ DES ACTIVITÉS DE LA MRC, DES MUNICIPALITÉS ET DES ORGANISMES MUNICIPAUX

La MRC, les municipalités et les organismes municipaux doivent disposer de mesures d'urgence issues de son plan de Continuité des services, lesquelles doivent être consignées par écrit, éprouvées et mises à jour en vue d'assurer la remise en service (dans un délai raisonnable) des systèmes d'information jugés essentiels en cas de sinistre majeur (ex. : incendie, attaque cybernétique, panne électrique prolongée, inondation, malveillance, etc.).

L'élaboration d'un plan de relève est prévue pour 2016 et son implantation s'effectuera au cours des deux années suivant son adoption par le Conseil de la MRC.

3.6. SENSIBILISATION ET FORMATION

Chaque gestionnaire au sein de la MRC, des municipalités et des organismes municipaux ayant accès aux actifs informationnels de la MRC, doit sensibiliser son personnel à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité ainsi qu'au rôle et aux obligations de tous les employés de son unité administrative dans le processus de protection de ces actifs. Le gestionnaire doit également veiller à ce que le personnel soit formé sur les Procédures de sécurité et sur l'utilisation adéquate des actifs informationnels afin de minimiser les Risques de sécurité possibles.

3.7. DROIT ET REGARD

La MRC a un droit de regard sur l'utilisation des actifs informationnels reliés au Réseau de la MRC par tous les Utilisateurs de son Réseau.

Les circonstances pour lesquelles ce droit de regard peut être exercé doivent être clairement définies et diffusées auprès des Utilisateurs. Ce droit de regard sera exercé conformément à la législation, notamment la Charte canadienne des droits et libertés (L.R.C. (1985) c-42), la Charte des droits et libertés de la personne du Québec (L.R.Q.,c. C-12), la Loi sur l'accès aux documents des organismes publics et sur la protection des Renseignements personnels (L.R.Q.,c. A-2.1).

4. RÔLES ET RESPONSABILITÉS

4.1. LE DIRECTEUR GÉNÉRAL

Il est le premier responsable des actifs informationnels de la MRC et est nommé par le Conseil de la MRC. Le Conseil approuve la présente politique.

4.2. LE DÉTENTEUR DE L'ACTIF INFORMATIONNEL

La MRC :

- assure la sécurité d'un ou de plusieurs actifs informationnels, qu'ils leur soient confiés par le dirigeant de l'organisme ou par un tiers mandaté;

- s'implique dans l'ensemble des activités relatives à la sécurité, notamment l'évaluation des Risques, la détermination du niveau de protection visé, l'élaboration des contrôles non informatiques et, finalement, la prise en charge des Risques résiduels;

- s'assure que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement;

- détermine les règles d'accès aux actifs dont ils assument la responsabilité avec l'appui du responsable de la sécurité des actifs informationnels de l'organisme.

4.3. LES GESTIONNAIRES

Les principales responsabilités du gestionnaire à l'égard de la protection des actifs informationnels de la MRC sont, entre autres :

- d'informer et de sensibiliser son personnel quant aux dispositions de la présente politique et des modalités liées à sa mise en œuvre;

- de s'assurer que la Ressource informationnelle est utilisée en conformité avec les principes généraux et les autres exigences de la présente politique ainsi que les règlements et les Procédures qui en découlent;

- de répondre de l'utilisation faite par son personnel des actifs informationnels connectés au Réseau de la MRC;

- de voir à l'application des directives, des pratiques et des standards permettant de respecter la présente politique et les Procédures et les règlements qui en découlent;

- de s'assurer que le niveau de connaissance de l'environnement de la sécurité de l'information entourant l'utilisation des actifs informationnels de la MRC est à jour et exhaustif.

4.4. LE SERVICE DE SOUTIEN INFORMATIQUE

Assure la mise en application des exigences de sécurité des actifs informationnels de la MRC durant tout le Cycle de vie de l'information numérique. Ses principales responsabilités sont, entre autres :

- de proposer les orientations de sécurité de l'information et les communiquer au personnel de la MRC ainsi qu'aux municipalités et aux organismes municipaux;

- d'assurer la coordination des grands projets de sécurité;

- d'assurer la sécurité de l'information relevant de sa responsabilité et la mise en application des exigences de protection des actifs informationnels de la MRC durant tout le Cycle de vie de l'information numérique;

- d'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 des actifs informationnels;

- de fournir au Détenteur d'actifs le soutien et les conseils en matière de protection de leurs actifs informationnels et de maintenir en état les moyens techniques de sécurité pour s'assurer de leur conformité aux besoins de sécurité déterminés par le Détenteur d'actifs;

- d'assurer le bon fonctionnement des Réseaux électroniques et des équipements informatiques de la MRC ainsi que de la connexion reliant la MRC aux Réseaux des municipalités et des organismes municipaux;

- d'informer immédiatement le directeur général adjoint de la MRC ou, en son absence, le directeur général, lorsqu'il constate qu'un Utilisateur déroge à la présente politique et d'en informer le gestionnaire.

4.5. LES UTILISATEURS

Tous les Utilisateurs sont responsables de respecter la présente politique ainsi que les règlements et les Procédures en vigueur en matière de sécurité de l'information et d'informer le service de soutien informatique de toute violation des mesures de sécurité dont ils pourraient être témoins ou de toute anomalie décelée pouvant nuire à la protection des actifs informationnels. À cet effet, ils :

- prennent connaissance et adhèrent à la politique globale de sécurité de l'information;

- utilisent les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et à l'intérieur des accès qui leur sont autorisés, comme défini dans le Règlement sur l'utilisation et la gestion des actifs informationnels;

- se conforment aux Procédures et aux règlements établis et dans le respect des dispositions de la présente politique.

5. DISPOSITIONS FINALES

5.1. RÉVISION

La présente politique est en vigueur et remplace la Politique sur l'utilisation des Réseaux électroniques, du courrier électronique, des médias sociaux ainsi que des équipements informatiques de la MRC de Pierre-De Saurel adoptée par résolution numéro 2013-02-28 du Conseil de la MRC lors de la séance ordinaire du 13 février 2013.

Afin d'assurer son adéquation aux besoins de sécurité de la MRC, la présente politique doit être régulièrement révisée et mise à jour lors de changements qui pourraient l'affecter.

5.2. MISE EN APPLICATION ET SUIVI DE LA POLITIQUE

Le responsable nommé par le Conseil de la MRC est chargé de l'application de la présente politique. Les Utilisateurs des actifs informationnels de la MRC doivent signer une entente avant qu'ils soient autorisés à accéder au Réseau.

Les ententes doivent être revues avec les Utilisateurs lorsqu'il y a un changement dans leur statut d'emploi ou leur contrat.

Les ententes des Utilisateurs doivent être conservées par le gestionnaire concerné, alors que les ententes des gestionnaires doivent être conservées par le Détenteur.

5.3. DATE D'ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son approbation par le Conseil de la MRC de Pierre-De Saurel.

ANNEXE 1 LOIS GÉNÉRALES

QUÉBEC. ***Code des professions, L.R.Q., c. C-26*****;**

CANADA. ***Code criminel, L.R.C. 1985, c. C-46*****;**

QUÉBEC. ***Code civil du Québec, L.R.Q., c. C-1991 (art. 35 à 41)*****;**

QUÉBEC. ***Charte des droits et libertés de la personne, L.R.Q., c. C-12 (art. 5 et 44)*****;**

QUÉBEC. ***Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1*****;**

QUÉBEC. ***Loi sur la sécurité civile, L.R.Q., c. S-2.3*****;**

QUÉBEC. ***Code municipal du Québec, L.R.Q., c. C-27.1 (art. 437.2)*****;**

QUÉBEC. ***Loi sur les cités et villes, L.R.Q., c. C-19 (art. 52)*****;**

QUÉBEC. ***Loi sur les normes du travail, L.R.Q., c. N-1.1*****;**

QUÉBEC. ***Loi sur l'éthique et la déontologie en matière municipale, L.R.Q., c. E-15.1.0.1*****;**

QUÉBEC. ***Loi sur les compétences municipales, L.R.Q., c. C-47-1*****;**

QUÉBEC. ***Loi sur l'équité salariale, L.R.Q., c. E-12.001*****;**

QUÉBEC. ***Loi sur les archives, L.R.Q., c. A-21.1*****;**

QUÉBEC. ***Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1*****;**

CANADA. ***Loi sur le droit d'auteur, L.R.C. (1985), c. C-42*****.**

ANNEXE 2 RÉFÉRENCES

***Politique portant sur l'utilisation des réseaux électroniques, du courrier électronique, des médias sociaux ainsi que des équipements informatiques de la municipalité régionale de comté de Pierre-De Saurel*, MRC de Pierre-De Saurel, 2013.**

***Guide pour l'élaboration d'une politique de sécurité de l'information numérique et des échanges électroniques*, gouvernement du Québec, 2003.**

***Guide de rédaction d'une politique de sécurité de l'information*, gouvernement du Québec, 2003.**

***Politique sur l'acceptation acceptable des dispositifs et des réseaux*, Secrétariat du Conseil du Trésor du Canada, 2013;**

***Politique sur la gestion de l'information*, Secrétariat du Conseil du Trésor du Canada, 2007;**

***Politique sur la sécurité du gouvernement,* Secrétariat du Conseil du Trésor du Canada, 2009;**

***Gestion de la sécurité des technologies de l'information*, Secrétariat du Conseil du Trésor du Canada;**

ROBERT, Jean-Marc*. Politiques de sécurité*, École de technologie supérieure.

***Politique de sécurité de l'information*, École de technologie supérieure, 2007.**

***Politique sur la sécurité informatique*, Université du Québec à Montréal, 2005.**

***Politique de sécurité sur les technologies de l'information et des télécommunications*, Université Laval, Québec, 1998.**

Textes
Alexandre Vovan
Vovan Tucker S.E.N.C.

Lecture et approbation
Patrick Delisle
Jacinthe Vallée
Caroline Morrison

Révision linguistique
Chantal Chapdelaine

Graphisme (seulement pour version graphique)
Éric Boulay
Vovan Tucker S.E.N.C.