MRC DE Pierre-De Saurel

RÈGLEMENT NUMÉRO 250-16

CONCERNANT L'UTILISATION ET LA GESTION DES ACTIFS INFORMATIONNELS DE LA MUNICIPALITÉ RÉGIONALE DE COMTÉ (MRC) DE PIERRE-DE SAUREL

VERSION REFONDUE

(incluant les dispositions des règlements numéros 297-18 et 308-19)

ATTENDU que la MRC de Pierre-De Saurel 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 d'information;

ATTENDU que la MRC a adopté le règlement numéro 249-16 édictant la Politique globale de sécurité de l'information de la MRC de Pierre-De Saurel;

ATTENDU qu'il y a maintenant lieu d'adopter un règlement, ainsi qu'un code de conduite permettant de régir l'utilisation et la gestion des actifs informationnels de la MRC;

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 Louis R. Joyal, appuyé par M. le Conseiller régional Jean-François Villiard et résolu à l'unanimité, que le présent règlement numéro 250-16 soit adopté et qu'il soit décidé 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 de régir l'utilisation et la gestion des actifs informationnels de la MRC et d'adopter un code de conduite (Annexe A) pour l'ensemble des utilisateurs du réseau de la MRC, le tout conformément à la Politique globale de sécurité de l'information de la MRC (réf. règlement numéro 249-16).

Article 3 - Sécurité de l'identifiant et l'authentifiant

Tout utilisateur est tenu de préserver la confidentialité de son mot de passe et d'en protéger l'accès et l'utilisation. Il doit donc s'assurer de ne pas le divulguer, intentionnellement ou non, à qui que ce soit. La MRC recommande fortement de ne pas conserver ces renseignements par écrit et de contacter le service de soutien informatique en cas d'oubli.

L'utilisateur est réputé imputable des activités entreprises par le biais de ses codes d'accès (identifiants) et de ses mots de passe (authentifiants). Il ne doit alors pas en divulguer la teneur à une tierce partie sans ensuite le modifier rapidement de façon confidentielle. Il est également responsable de restreindre l'accès à des tierces parties aux ordinateurs et autres dispositifs d'accès authentifiés au réseau grâce à ses identifiants et authentifiants.

L'utilisateur doit s'assurer que l'authentifiant, lorsqu'il peut le choisir, respecte minimalement les normes de sécurité informatique de la MRC propres aux actifs informationnels qu'il utilise.

Article 4 - Autorisations d'accès aux actifs informationnels

4.1 Accès local

Tout utilisateur doit posséder un identifiant, un authentifiant et des autorisations spécifiques à ceux-ci lorsqu'il se voit attribuer un accès local au réseau. Les autorisations qui lui sont attribuées lui donnent accès aux actifs informationnels de la MRC dépendamment de ses fonctions de travail ou des spécificités de sa collaboration avec la MRC.

Tout utilisateur peut demander un accès spécifique aux actifs informationnels de la MRC, en plus de l'accès de base qui lui est accordé, en acheminant une requête détaillée au service de soutien informatique. L'autorisation lui sera accordée si sa demande est approuvée par le directeur général adjoint de la MRC ou, en son absence, par le directeur général de la MRC.

4.2 Transfert de fichiers (réf. règlement numéro 308-19)

Les utilisateurs ne doivent pas utiliser leur adresse courriel professionnelle pour transmettre des fichiers de plus de 5 mégaoctets.

Plusieurs moyens sont disponibles gratuitement afin de partager des documents volumineux.

À titre d'exemple, les utilisateurs peuvent utiliser WeTranfer, Google drive, Microsoft One Drive, DropBox, etc. conformément à la Politique globale de sécurité de l'information MRC de Pierre-De Saurel.

4.3 Accès à distance (réf. règlement numéro 308-19)

L'accès à distance, différemment au transfert de fichiers, permet à un utilisateur de se connecter au réseau à partir d'un lieu autre que les locaux physiques constituant le réseau local de la MRC ou des municipalités ou des organismes municipaux et d'avoir les mêmes autorisations d'accès et d'utilisation des actifs informationnels au même titre que s'il était connecté au réseau à partir du réseau local de la MRC.

La seule méthode d'accès à distance permise est celle par connexion VPN. Celle-ci permet à l'utilisateur de faire partie du réseau local de la MRC virtuellement, c'est-à-dire à partir d'un lieu autre que les locaux physiques de la MRC.

Toute autre méthode d'accès à distance telle que LogMeIn, Ammy, TeamViewer, etc. doit uniquement être utilisée pour le soutien à distance de la part de fournisseurs externes ou par le service de soutien informatique de la MRC de Pierre-De Saurel.

Toute demande d'autorisation pour l'accès à distance au réseau doit être acheminée au service de soutien informatique avec une description détaillée des besoins. Une fois la demande approuvée par le gestionnaire, le service de soutien informatique procédera à la configuration de l'infrastructure VPN du réseau local de la MRC afin de donner les accès et les autorisations nécessaires à l'utilisateur. Un guide sera fourni à l'utilisateur pour qu'il puisse installer et configurer le logiciel nécessaire sur son ordinateur ou un dispositif d'accès.

Article 5 - Conditions d'utilisation des actifs informationnels

5.1 Usage prohibé

L'utilisation des actifs informationnels de la MRC est limitée à la réalisation de la mission prévue de ces actifs et au respect des droits et des responsabilités des autres utilisateurs. Les utilisateurs du réseau sont tenus de se conformer au présent règlement, à toutes les politiques, code de conduite et code d'éthique.

À moins d'une autorisation par les responsables des actifs informationnels en cause, l'utilisateur ne doit pas poser ou tenter de poser l'un des gestes suivants :

- prendre connaissance, modifier, détruire, déplacer ou divulguer de façon non autorisée des actifs informationnels;
- lire, modifier ou détruire tout message, texte, donnée ou logiciel sans l'autorisation de son propriétaire ou du responsable des actifs informationnels concerné;
- utiliser, décrypter ou décoder un code ou une clé d'accès, de fichier ou de mot de passe sans autorisation préalable du responsable de ces ressources;
- utiliser les actifs informationnels de façon abusive ou nuisible au bon fonctionnement;
- contourner les mécanismes de protection des actifs informationnels;
- ne pas respecter la réglementation des réseaux externes auxquels la MRC a accès (évaluation municipale, service de sécurité incendie, etc.), ni l'Intégrité des systèmes informatiques ainsi accessibles;
- utiliser les actifs informationnels de la MRC à des fins commerciales non autorisées ou illicites;
- propager du matériel utilisant un langage injurieux, malveillant, haineux ou discriminatoire ainsi que de toute forme de harcèlement, de menace ou de diffamation;
- consulter et propager tout fichier, document ou message considéré comme étant diffamatoire, offensant, harcelant, discriminatoire, violent, raciste, à connotation sexuelle, politique, religieuse, etc.;
- voler les ressources et/ou les utiliser de façon malicieuse ou contraire aux lois et règles d'éthique en vigueur;
- installer, copier ou emprunter les logiciels enregistrés sous une licence au nom de la MRC de Pierre-De Saurel;
- installer ou télécharger un logiciel ou modifier la configuration du système d'exploitation (structure interne et thématique visuelle) d'un ordinateur relié au réseau sans l'autorisation préalable du service de soutien informatique avec l'approbation du gestionnaire;
- diffuser de l'information confidentielle ou protégée par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q. c. A-2.1);
- rédiger ou envoyer tout commentaire, courriel ou message ayant pour but de nuire à la réputation ou visant à entraver d'une quelconque façon la bonne marche des activités de la MRC ou de l'un des organismes municipaux ou de ses municipalités;
- ne pas informer le service de soutien informatique de la MRC à la suite de l'infection d'un système informatique par un virus, d'une altération illicite ou d'un bris.

L'installation, le déplacement, la désinstallation ou l'utilisation d'un équipement de télécommunications (par exemple : routeur, point d'accès Wi-Fi, passerelle, commutateur, etc.) sur le réseau doit être approuvé par le service de soutien informatique.

Cette approbation a pour but de mieux cerner les besoins de l'utilisateur, de l'informer des conséquences de l'utilisation d'équipement de télécommunication et, au besoin, de lui proposer d'autres solutions dans le cas où l'utilisation d'un de ces équipements pourrait affecter la qualité du service du réseau.

5.2 Usage personnel

Les utilisateurs peuvent faire un usage raisonnable de certains actifs informationnels à des fins personnelles, par exemple pour le traitement de renseignements qui leur sont personnels et qui ont un caractère confidentiel, à la condition que cet usage soit conforme aux dispositions de ce règlement.

Dans certains cas, l'utilisation des actifs informationnels à des fins personnelles, par exemple l'utilisation du réseau et des ordinateurs publics pour l'échange de fichiers ou le clavardage, peut faire l'objet de restrictions ou d'interdictions par le gestionnaire concerné.

L'utilisation des actifs informationnels de la MRC ne doit en aucun temps être une source de travail additionnel pour le service de soutien informatique de la MRC.

La tolérance d'utilisation à des fins personnelles peut être retirée par le gestionnaire s'il juge qu'il y a abus ou que telle utilisation est incommodante.

L'utilisation à des fins personnelles ne rend pas nécessairement les communications ou le contenu de tout fichier privé ou confidentiel. Le droit à l'utilisation personnelle n'a pas pour effet d'empêcher l'accès à un actif informationnel par une personne autorisée, autre que son utilisateur principal, lorsque cet accès est requis par la nécessité du service et qu'il est autorisé par le gestionnaire.

5.3 Protection des ordinateurs et autres dispositifs d'accès

L'utilisateur doit assurer la sécurité des ordinateurs et autres dispositifs d'accès aux actifs informationnels qu'il utilise ou dont il est responsable.

Tout utilisateur des actifs informationnels de la MRC doit s'assurer que le dispositif d'accès qu'il utilise, ou dont il est responsable, est protégé contre tout virus et autres logiciels pernicieux. Ce même dispositif doit également être protégé contre les failles corrigibles de sécurité des systèmes ou des applications utilisées, dans le respect des normes établies pour ces systèmes.

Tout utilisateur ou responsable des dispositifs d'accès au réseau doit garantir la protection physique de ces équipements en mettant en place des mesures appropriées.

5.4 Droits de propriété intellectuelle

En tout temps, l'utilisateur doit respecter les lois fédérales sur les brevets, le droit d'auteur et les marques de commerce en vigueur ainsi que les ententes contractuelles avec les fournisseurs de contenu.

La reproduction de logiciels, de progiciels ou de didacticiels n'est autorisée qu'à des fins de copies de sécurité ou selon les normes institutionnelles de la licence d'utilisation la régissant. Il est strictement interdit aux utilisateurs de :

- reproduire ou utiliser toute reproduction illicite d'un logiciel, d'un fichier électronique ou de la documentation qui y est jointe;
- participer directement ou indirectement à la reproduction illicite d'un logiciel ou d'un fichier électronique;
- consulter, modifier ou détruire un logiciel ou une banque de données sans l'autorisation de la détentrice ou du détenteur des droits;
- utiliser les actifs informationnels afin de commettre ou tenter de commettre une infraction aux lois, en particulier les lois régissant la propriété intellectuelle.

Article 6 - Gestion et protection des actifs informationnels

6.1 Responsabilité

La responsabilité de chacun des actifs informationnels est formellement attribuée au gestionnaire dont l'identité et la portée des responsabilités en matière de protection de ces actifs sont communiquées au service de soutien informatique.

6.2 Gestion des droits d'accès

Tout actif informationnel contenant des renseignements confidentiels ou à accès restreint doit être protégé, au minimum, par un mécanisme d'identification et d'authentification de l'utilisateur. Ce mécanisme doit également permettre de limiter la divulgation, le traitement et la mise à la disposition des données et des systèmes aux seules personnes ou entités autorisées, selon les modalités établies.

L'octroi des droits d'accès doit être effectué par le biais d'une procédure établie par le service de soutien informatique et faire l'objet d'une autorisation formelle par le responsable identifié. Cette procédure doit notamment respecter le principe de moindre accès qui consiste à limiter l'accès au minimum de personnes requis par la nécessité du service et à ne rendre accessibles que les seules données pertinentes à l'exercice de leur fonction et non l'ensemble des données.

6.3 Protection des actifs informationnels

Le gestionnaire des actifs informationnels doit effectuer une évaluation des risques inhérents aux actifs dont il a la charge. Pour ce faire, il doit être assisté par le service de soutien informatique afin de cerner adéquatement les besoins de sécurité en matière de confidentialité, d'intégrité et de disponibilité de l'actif.

Le gestionnaire de systèmes est également responsable de s'assurer de la mise en œuvre des moyens nécessaires pour combler les besoins de sécurité informatique.

Article 7 - Gestion des problèmes et des incidents de sécurité informatique

7.1 Communication 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, au directeur général, de tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité telle que le vol, l'intrusion dans un réseau ou système, les dommages délibérés, l'utilisation abusive, la fraude, etc.

Cette personne doit également aviser le service de soutien informatique de l'incident, et ce, même si elle considère que la situation est résolue.

Les utilisateurs doivent également collaborer, dans la limite où cette collaboration ne leur portera pas un préjudice personnel, avec le service de soutien informatique dans le cadre des exercices d'évaluation de la sécurité informatique et des enquêtes lors d'incidents de sécurité informatique.

7.2 Mesures d'urgence

Afin de préserver l'intégrité des services des actifs informationnels, le service de soutien informatique peut, après avoir pris les moyens raisonnables pour aviser les responsables ou utilisateurs des actifs informationnels, poser les actions suivantes ou exiger qu'elles soient posées :

- interrompre ou révoquer temporairement les services offerts à certains utilisateurs afin de protéger le reste des utilisateurs;
- intervenir sur un actif informationnel suspecté de contrevenir à l'une ou l'autre des dispositions prévues dans le présent règlement;
- appliquer les différentes fonctions de diagnostic sur les actifs informationnels;
- prendre les mesures urgentes requises afin de circonscrire la situation.

7.3 Contrôle, vérification et vie privée

Dans le cadre des activités de contrôle et de vérification, le gestionnaire a l'obligation de respecter la dignité, la liberté d'expression, la liberté de pensée et la vie privée des membres de la communauté.

Le service de soutien informatique est autorisé à procéder à toutes les vérifications d'usage estimées nécessaires pour s'assurer du respect des dispositions de ce règlement et du code de conduite, ainsi que des politiques, des procédures et du code d'éthique pertinents ou des lois et des règlements provinciaux et fédéraux.

Une vérification nominative des renseignements personnels et privés d'un utilisateur ou de son utilisation des actifs informationnels ne peut être effectuée sans le consentement de cette personne, à moins que le gestionnaire ait des motifs valables de croire que cette dernière contrevient à l'une ou l'autre des dispositions du présent règlement ou du code de conduite.

L'utilisation de la technologie dans les activités de contrôle et de vérification ne peut pas permettre que soient surveillés, sans motifs valables, les faits et gestes des utilisateurs ou le contenu de leurs communications.

Cette restriction ne s'applique cependant pas aux activités de journalisation automatique par des logiciels, lesquels sont nécessaires pour assurer la pérennité des services aux utilisateurs du réseau. C'est alors la consultation et l'interprétation de données nominatives qui ne peuvent être faites sans motif valable, conformément au processus de vérification décrit ci-dessous.

Dans le cas d'une vérification qui implique l'accès à des données privées et confidentielles, que ces données soient l'objet ou non de la vérification, le gestionnaire doit veiller à éviter toute surveillance ou tout contrôle abusif. Le gestionnaire ne peut vérifier que lorsqu'il possède des motifs valables de croire qu'un utilisateur manque à ses obligations ou abuse des outils qui lui sont fournis.

Dans l'éventualité où une vérification nominative des informations personnelles et privées d'un utilisateur ou de son utilisation des actifs informationnels a été effectuée et que l'ensemble du processus de vérification et des activités qui en découlent est complété, l'utilisateur doit être informé de la vérification qui a eu lieu et des renseignements qui ont été consultés dans ce cadre.

Article 8 - Responsabilité de la MRC

La MRC, les municipalités et les organismes municipaux sont responsables de fournir les ressources nécessaires aux utilisateurs du réseau afin qu'ils puissent assumer leurs responsabilités quant à la sécurité informatique, et ce, dans un cadre de saine gestion des risques pour la MRC. Cependant, la MRC ne peut pas être tenue responsable des pertes, des dommages, des manques à gagner ou des inconvénients qui pourraient être causés à une personne, physique ou morale, à l'occasion ou en conséquence de l'utilisation des actifs informationnels de la MRC ou advenant le cas où elle devrait, pour quelque cause que ce soit, diminuer ses services, ou les interrompre, quelle que soit la durée de telles diminutions ou interruptions.

Article 9 - Abrogation

Le présent règlement abroge et remplace tout règlement, résolution, politique ou directive portant sur l'utilisation et la gestion des actifs informationnels de la MRC.

Article 10 -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 – Code de conduite des utilisateurs du réseau de la MRC de Pierre-De Saurel

AVIS DE MOTION : 14 octobre 2015
ADOPTION : 20 janvier 2016
ENTRÉE EN VIGUEUR : 19 février 2016

MRC DE Pierre-De Saurel

CODE DE CONDUITE

DES UTILISATEURS DU RÉSEAU DE LA MRC DE PIERRE-DE SAUREL

Présentation

Le présent « Code de conduite » est adopté en vertu du règlement numéro 249-16 édictant la Politique globale de sécurité de l'information de la MRC de Pierre-De Saurel.

En vertu des dispositions de cette politique, la MRC adopte par règlement un code de conduite pour tous les utilisateurs de son réseau, lequel encadre la gestion quotidienne de l'utilisation du réseau et précise les règles de bonnes pratiques pour l'ensemble des utilisateurs.

1. Respect d'autrui

Toute personne a droit au respect de sa vie privée et de sa réputation.

2. Respect de la propriété intellectuelle

Par propriété intellectuelle (PI), on entend un droit juridique à une idée, à une invention ou à une création des domaines industriel, scientifique, littéraire et artistique. La PI englobe aussi les droits d'auteurs, les marques de commerce, les symboles, les noms, les images, les dessins industriels et les modèles à usage commercial. L'utilisation de la PI est soumise aux lois fédérales sur les brevets, le droit d'auteur et les marques de commerce.

3. Utilisation autorisée

Tout utilisateur doit utiliser le réseau avec soin et respect.

Tout utilisateur du réseau doit au préalable s'identifier et signer une entente dans laquelle il s'engage à respecter le présent code.

Lorsqu'il constate une défaillance des équipements informatiques ou du réseau, l'utilisateur doit rapporter immédiatement l'existence de tout virus, altération illicite ou bris au service de soutien informatique, qui, lui, doit aviser sans délai le gestionnaire. L'utilisation des équipements informatiques à des fins personnelles ne doit en aucun temps être une source de travail additionnel pour le service de soutien informatique de la MRC.

3.1 Employés de la MRC

Tout utilisateur qui est employé de la MRC reconnait que l'équipement informatique mis à sa disposition est avant tout un outil de travail. L'utilisation occasionnelle à des fins personnelles est permise pourvu que cela n'entrave pas le travail habituel et normal de l'utilisateur, ni celui des autres utilisateurs, qu'elle se fasse en dehors des heures régulières de travail ou pendant une période de pause et qu'elle soit d'une durée limitée.

La tolérance d'utilisation à des fins personnelles peut être retirée par le directeur général adjoint ou, en son absence, par le directeur général, s'il juge qu'il y a abus ou que telle utilisation est incommodante.

3.1.1 Courrier électronique

L'utilisateur doit rédiger ses courriels avec le plus grand soin. Les courriels sont traités comme des documents et, selon leur degré d'importance, font partie des archives de la MRC.

3.1.2 Équipements informatiques

L'utilisateur doit utiliser les ressources matérielles et les logiciels pour lesquels les droits ou les autorisations ont été obtenus par la MRC. Par conséquent, il est interdit d'installer ou d'utiliser tout logiciel ou démo, de télécharger tout logiciel, démo ou fichier n'ayant pas trait directement à l'usage normal aux fins du travail de l'utilisateur. L'installation de logiciel par quelque moyen que ce soit est conditionnelle à l'autorisation du service de soutien informatique de la MRC.

3.1.3 Médias sociaux

On entend par « médias sociaux » les sites Web qui permettent aux utilisateurs d'échanger des commentaires, des photos et des opinions, tels que Facebook, Twitter, Linkedin, MySpace et YouTube.

Aucun utilisateur ne peut parler au nom de la MRC, à moins d'y être autorisé. Dans certaines circonstances, la MRC peut exiger la modification ou le retrait d'un élément communiqué sur un média social.

La communication de renseignements, même s'ils peuvent sembler anodins ou qu'ils préservent l'anonymat de la MRC, peut quand même constituer un manquement à l'obligation de confidentialité de l'utilisateur.

4. Usage prohibé

4.1 Pour l'ensemble des utilisateurs

Les usages suivants sont non autorisés et inacceptables (liste non exhaustive) :

- Le visionnement, le transfert et la communication de tout fichier, document, message ou la navigation sur des sites dont le contenu est ou peut être considéré comme étant diffamatoire, offensant, harcelant, discriminatoire, violent, raciste, à connotation sexuelle, politique, religieuse, etc.;
- L'utilisation du réseau ou l'envoi de messages de nature à générer une surutilisation du trafic ou d'affecter d'une autre manière le travail des autres utilisateurs (ex. écouter la radio sur Internet, visualiser des vidéos ou des séries sur YouTube, Tou.tv, etc.);
- L'envoi de messages anonymes (tout message ou document doit indiquer sa provenance ou être signé);
- L'envoi de message de masse sans mettre les destinataires en copie conforme invisible;
- L'utilisation du courriel « xx@pierredesaurel.com » à des fins autres que professionnelles;
- L'ouverture d'une pièce jointe d'un courriel dont le destinataire n'est pas connu de l'utilisateur (en cas d'incertitude, contacter le service de soutien informatique de la MRC);
- La diffusion d'information confidentielle ou protégée par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L. R. Q. c. A-2.1);
- Tout commentaire, courriel ou message ayant pour but de nuire à la réputation ou visant à entraver d'une quelconque façon la bonne marche des activités de la MRC ou de l'une de ses municipalités;
- L'installation ou le téléchargement d'un logiciel, d'un fichier ou d'une icône sans l'autorisation du service de soutien informatique de la MRC;
- L'utilisation, sans autorisation, du code ou du mot de passe d'un autre utilisateur.
- Le fait d'endommager, altérer ou perturber le fonctionnement des systèmes informatiques par négligence ou volontairement ou de ne pas informer le service de soutien informatique de la MRC à la suite de l'infection du système informatique par un virus.

4.2 Pour les employés de la MRC (réf. : Règlement 297-18)

Les usages suivants sont non autorisés et inacceptables (liste non exhaustive) :

- La consommation de jeux informatiques (ex. dame de pique, solitaire, poker, démineur, course, etc.);
- Les groupes de discussions (chat) sur Internet ou autre support ou accès (ex. MSN, Facebook, etc.) utilisés à des fins autres que professionnelles;
- L'installation, la copie ou l'emprunt de logiciels enregistrés sous une licence au nom de la MRC;
- L'utilisation du courriel « xx@mrcpierredesaurel.com » à des fins autres que professionnelles;

Le fait de quitter son poste de travail sans verrouiller préalablement sa session de travail.

5. Responsabilité de l'utilisateur

Chaque utilisateur est légalement responsable de toute communication effectuée dans les médias sociaux et devrait, en tout temps, respecter la législation en vigueur.

6. Responsabilité de la MRC

Le service de soutien informatique est responsable du bon fonctionnement du réseau et des équipements informatiques de la MRC. Lorsqu'il constate qu'un utilisateur déroge à la présente politique, il doit immédiatement en informer le gestionnaire ainsi que le directeur général adjoint de la MRC ou, en son absence, le directeur général.

De plus, toute personne ayant connaissance d'un manquement au présent Code peut, de façon confidentielle, porter plainte au gestionnaire, qui doit en aviser le directeur général adjoint de la MRC ou, en son absence, le directeur général.

7. Autres dispositions applicables à certains utilisateurs

Certains utilisateurs doivent se rappeler qu'ils sont soumis à différents règlements et code d'éthique, lesquels continuent de s'appliquer à toute communication et restreignent ou interdisent la communication de certains renseignements tant à propos de l'employeur en général que des collègues, de la direction et des membres du Conseil.

8. Mesures de contrôle

La MRC se réserve le droit de prendre les mesures raisonnables et appropriées dans le but de superviser et contrôler l'utilisation faite des équipements informatiques et du réseau mis à la disposition des utilisateurs et de déterminer si ces équipements et ce réseau sont utilisés conformément au présent code.

9. Sanction

Toute plainte au regard du présent code doit :

1° Être déposée sous pli confidentiel au directeur général adjoint de la MRC ou, en son absence, au directeur général, qui verra, le cas échéant, à déterminer s'il y a eu contravention au présent code;

2° Être complète, écrite, motivée et accompagnée, s'il y a lieu, de tout document justificatif.

À l'égard du directeur général adjoint, toute plainte doit être déposée au directeur général de la MRC. Les paragraphes 1° et 2° ci-dessus s'appliquent en faisant les adaptations nécessaires.

À l'égard du directeur général, toute plainte doit être déposée au préfet de la MRC. Les paragraphes 1° et 2° ci-dessus s'appliquent en faisant les adaptations nécessaires.

9.1 Pour une plainte visant un utilisateur, autre qu'un employé de la MRC

Toute violation aux règles contenues au présent code peut entraîner la révocation du privilège d'accès à l'utilisateur. Le gestionnaire a la responsabilité de s'assurer que la révocation du privilège d'accès est appliquée. En cas d'omission du gestionnaire, l'organisme municipal pourra se voir retirer l'accès au réseau.

Dans le cas d'un manquement à une obligation qui s'applique à un utilisateur qui n'est pas un employé de la MRC ou lorsque ce manquement survient après la fin du contrat de travail d'un ancien employé, la MRC accepte que tout désaccord ou différend relatif au code de conduite ou découlant de son interprétation ou de son application soit soumis à une médiation. Le médiateur sera choisi de concert par les parties impliquées. Si aucune entente n'intervient dans les 60 jours suivant la nomination du médiateur, ce différend sera tranché de façon définitive par voie d'arbitrage et à l'exclusion des tribunaux, selon les lois du Québec. Les parties pourront à tout moment convenir d'un délai plus long avant de soumettre le différend à l'arbitrage.

À moins que les parties n'en décident autrement dans une convention d'arbitrage, l'arbitrage se déroulera sous l'égide d'un arbitre seul et sera conduit conformément aux règles de droit et aux dispositions du Code de procédure civile du Québec en vigueur au moment de ce différend. La sentence arbitrale sera finale, exécutoire et sans appel et liera les parties.

9.2 Pour une plainte visant un employé de la MRC

Toute violation aux règles contenues au présent code peut entraîner non seulement la suspension, la modification ou la révocation du privilège d'accès, mais également, pour les employés, l'inscription de mesures administratives ou disciplinaires pouvant aller jusqu'au congédiement.

La MRC reconnaît l'aspect correctif de la discipline en milieu de travail. Elle reconnaît que la mesure disciplinaire imposée sera juste et raisonnable, et proportionnelle à la gravité de la faute reprochée.

Aucune sanction ne peut être imposée à un employé sans que ce dernier :

1° ait été informé, par écrit, des motifs et des faits qui sont à l'origine de la décision du Conseil de la MRC ou du directeur général;

2° ait eu l'occasion d'être entendu.