Edmundston

POLITIQUE ADMINISTRATIVE	**No. 24**
ACCÈS SÉCURISÉS DES BÂTIMENTS MUNICIPAUX	Résolution # 2011-018 Adoptée le: 15 mars 2011

1 OBJECTIFS

1.1 Cette politique vise :

- à rehausser la sécurité dans les bâtiments municipaux;
- à y contrôler les accès; et
- à protéger les locaux, les équipements, le matériel, les dossiers, les informations et les personnes qui se trouvent à l'intérieur.

1.2 Cette politique précise les règles et modalités que les utilisateurs du système d'accès sécurisé doivent respecter concernant les équipements mis à leur disposition dans le cadre de leurs fonctions et a aviser les utilisateurs de l'existence des mesures de sécurité qui les entourent;

1.3 L'application de cette politique requiert la collaboration de l'ensemble du personnel de la municipalité et de toute autre personne qui utilise les édifices municipaux.

2 TERMINOLOGIE

2.1 Zones d'accès sécurisées

L'expression « zone sécurisée » peut s'appliquer à n'importe quel ensemble de zones restreintes, par exemple, à un regroupement de zones restreintes séparées par des zones publiques ou des zones d'accueil. Les diverses zones sont définies comme suit :

a) La **zone publique** entoure l'installation de la municipalité ou en fait partie. Exemples : terrain entourant un immeuble; couloirs ou corridor principal et halls d'ascenseurs dans les immeubles et les accès aux personnes handicapées.

b) La **zone d'accueil** se trouve généralement à l'entrée de l'immeuble où se fait le contact initial entre le public et la municipalité et où l'on fournit les services et les renseignements. L'accès peut être limité à certaines heures de la journée ou pour des raisons déterminées.

c) Une **zone de travail** doit être délimitée par un périmètre facile à reconnaître et faire l'objet d'une surveillance périodique. C'est l'endroit où commence la sécurisation de l'accès. Exemple : bureaux en aire ouverte ou local électrique.

d) Une **zone de sécurité** doit être délimitée par un périmètre facile à reconnaître et être surveillée en permanence. Exemples : lieux où des renseignements confidentiels sont traités, salle des serveurs informatiques, archives et voûtes.

e) Une **zone de haute sécurité** doit être délimitée par un périmètre construit selon des spécifications spéciales et être surveillée en permanence. L'accès à une telle zone doit être sécurisée et vérifié. Exemples : salles d'interrogatoire, cellules, salles d'exhibit, etc.

3 PERSONNES VISÉES PAR LA POLITIQUE

La présente politique s'applique aux personnes suivantes:

a) Tous les employés municipaux;

b) Toute personne qui doit accéder aux bâtiments dans le cadre d'un contrat, d'un échange de services, d'un mandat, d'un stage, d'une collaboration ou autres;

c) Toute personne à laquelle une carte d'accès a été attribuée;

d) Tous les fournisseurs et tous les autres visiteurs incluant les sous-traitants, les clients et toutes autres personnes utilisant les bâtiments municipaux ;

e) Tous les membres du conseil municipal.

4 ÉNONCÉ DE POLITIQUE

4.1 Principe

Les personnes visées par la présente politique doivent agir avec discernement et de façon responsable lors de l'utilisation des outils d'accès sécurisé mis à leur disposition, et ce, en respectant la présente politique.

4.2 Confidentialité et vie privée

a) Aucune information personnelle sur les utilisateurs n'est contenue sur les cartes ou jetons d'accès;

b) Uniquement les informations personnelles requises pour l'opération du système d'accès sécurisé sont contenues dans le serveur principal du système d'accès sécurisé. Une photo de chaque utilisateur pourra être conservée dans ce dossier à titre d'identification. Ces informations sont protégées par le système de sécurité du système d'accès sécurisé ainsi que par la sécurité appliquée au réseau informatique de la municipalité.

4.3 Personnes responsables du système

a) Deux employés municipaux seront nommés pour agir à titre de « **gestionnaires principaux** » du système d'accès sécurisé en plus du personnel de la firme d'expert-conseil responsable de l'entretien du système;

b) Les gestionnaires principaux auront la responsabilité de:

   a. S'assurer que le système fonctionne selon les directives du fournisseur et le guide de procédures;
   b. Gérer, faire la formation et superviser les gestionnaires de secteur;
   c. Activer ou désactiver le système au besoin;
   d. Créer la base de données initiale
   e. Vérifier les rapports du système et rapporter les anomalies;
   f. Tenir informé la Direction générale du fonctionnement du système.

c) Deux personnes par service ou secteur d'activité seront mandatées pour agir à titre de « **gestionnaire de secteur** » du système d'accès sécurisé, sous la responsabilité de leur directeur respectif.

d) Les gestionnaires de secteur auront la responsabilité de:

   a. Activer ou désactiver les cartes ou jetons d'accès pour leur secteur ;
   b. Donner ou retirer des droits d'accès aux utilisateurs de leur secteur sur autorisation du directeur de service;
   c. Gérer les cartes ou jetons d'accès, si applicable;
   d. Gérer les horaires d'accès;
   e. Recevoir, générer et analyser les rapports du système et présenter les résultats au directeur du secteur;
   f. Référer à l'un des gestionnaires principaux pour tout besoin d'information ou aide sur l'opération du système;
   g. Créer les nouveaux utilisateurs et effectuer la mise à jour de leur secteur.

e) Les gestionnaires de secteur n'ont pas la possibilité de voir ou de modifier les informations sur les équipements et les usagers des autres secteurs de la municipalité.

4.4 Usages autorisés

Les outils du système d'accès sécurisé sont utilisés spécifiquement pour les activités suivantes:

a) Donner un accès sécuritaire au public;

b) Accès aux bâtiments et locaux municipaux requis dans le cadre de leurs fonctions durant les heures normales d'ouverture ou selon leurs horaires de travail;
   i. Les employés municipaux;
   ii. Les membres du conseil municipal ;

c) Sauf les exceptions identifiées ci-après, les employés qui doivent accéder aux locaux municipaux, les jours fériés et en dehors des heures normales d'ouverture ou de leur horaire de travail, doivent préalablement obtenir une autorisation de leur directeur de service.

d) Les personnes suivantes sont admises, pour des motifs reliés à leur fonction, 24 heures par jour et 7 jours par semaine à certains bâtiments municipaux, tels que définis dans le guide de procédures et déterminés comme suit:

i) les gestionnaires municipaux, tels que déterminés par le Directeur général;

ii) les personnes désignées par les gestionnaires principaux pour l'entretien du système d'accès sécurisés;

iii) les employés désignés par un Directeur de service qui peuvent être appelés à intervenir en tout temps;

iv) le maire et les conseillers municipaux, tels que déterminés par le conseil municipal.

4.5 Usages interdits

Il est strictement interdit de recourir aux outils du système d'accès sécurisé pour les usages suivants:

a) Prêter sa carte ou son jeton d'accès à une personne autorisée ou non;

b) Permettre l'accès à une personne non autorisée sans supervision;

c) Divulguer son code d'accès ou son NIP à une autre personne autorisée ou non;

d) Laisser pénétrer une personne autorisée à une zone sécurisée sans que celle-ci présente sa carte ou son jeton d'accès, si applicable;

e) Accéder ou tenter d'accéder à des locaux qui ne lui sont pas autorisés;

f) Bloquer ou tenter de bloquer intentionnellement le verrouillage d'une porte;

g) Créer ou tenter de créer intentionnellement des pannes ou des bris au système;

h) Utiliser ou tenter d'utiliser l'identité d'un autre individu;

i) Divulguer des informations sur le système d'accès sécurisé à une personne non autorisée ou à une personne non responsable de la gestion du système d'accès sécurisé;

j) Donner ou tenter de donner des droits d'accès à des personnes non autorisées;

k) Relier ou tenter de relier des équipements non autorisés au système;

l) Modifier, altérer ou endommager les cartes ou jetons d'accès ;

m) Utiliser ou tenter d'utiliser les cartes ou jetons d'accès à d'autres fins non autorisées par la municipalité;

n) Toute autre utilisation ou tentative d'utilisation pouvant mettre la sécurité des personnes ou des biens de la municipalité en danger.

4.6 Contrôle et vérification

a) L'utilisation des outils d'accès sécurisés de la municipalité est un privilège et non un droit acquis et l'autorisation de les utiliser peut être révoquée en tout temps;

b) Les outils d'accès sécurisés mis à la disposition des personnes visées par la présente politique, demeurent en tout temps la propriété exclusive de la municipalité;

c) Toute personne qui aura fait une utilisation inappropriée des outils d'accès sécurisés ou qui aurait déjoué ou tenté de déjouer le système pourra perdre son privilège de l'utiliser et pourra faire l'objet de mesures disciplinaires;

d) L'utilisateur des outils d'accès sécurisés sera tenu responsable de tous les dommages et frais que son comportement aura causé, incluant, mais ne s'y limitant pas, à un usage négligent ou abusif des équipements ayant causé des pertes ou des bris;

e) Le service des ressources humaines de la municipalité sera responsable des listes d'accès aux bâtiments municipaux et fera automatiquement suspendre les accès d'un employé ou d'une autre personne autorisée durant une période d'absence prolongée pour maladie ou pour suspension. Lors d'un départ définitif de l'organisation, les accès des personnes concernés seront immédiatement suspendus;

f) Les gestionnaires principaux, nommés en vertu de la présente politique, pourront vérifier, en tout temps, si l'utilisation des outils d'accès sécurisé respecte les directives de la présente politique ainsi que les valeurs organisationnelles de la municipalité, et ce, selon la procédure de vérification identifiée dans la présente politique;

g) Des rapports d'utilisation du système seront disponibles pour vérification, au besoin, au service des ressources humaines de la municipalité afin d'effectuer les suivis nécessaires auprès des personnes concernées.

4.7 Procédures de vérifications

Advenant le non-respect ou le doute de non-respect de la présente politique, les procédures suivantes sont applicables:

a) Lorsqu'une utilisation inappropriée est détectée par l'un des gestionnaires principaux:

i) Le gestionnaire principal ouvre un rapport de vérification, identifie le type d'utilisation inappropriée, effectue une vérification du dossier et recueille les détails pertinents;

ii) Le gestionnaire principal rapporte les faits par écrit au Coordonnateur(e) des ressources humaines;

iii) Le secteur des ressources humaines prend connaissance de toute utilisation inappropriée et avise le directeur du service et le directeur général qui déterminent conjointement la mesure disciplinaire qui s'applique.

b) Lorsqu'une utilisation inappropriée est détectée par toute autre personne visée par la présente politique :

i) Un avis est émis dans les plus brefs délais à son superviseur-cadre en indiquant la date et le type d'utilisation inappropriée détectée;

ii) Le superviseur-cadre avise immédiatement le directeur du service et le Coordonnateur(e) des ressources humaines;

iii) Le service des ressources humaines avise un des gestionnaires principaux qui ouvre un rapport de vérification, identifie le type d'utilisation inappropriée, effectue une vérification du dossier et recueille les détails pertinents et avise le service des ressources humaines du résultat;

iv) Le secteur des ressources humaines avise le directeur du service et le directeur général de toute utilisation inappropriée et détermine conjointement la mesure disciplinaire qui s'applique.

c) **Lorsqu'une utilisation inappropriée est effectuée par un élu, un client, un fournisseur, un visiteur ou toute autre personne visée par la présente politique:**

i) un avis est immédiatement émis au directeur général ou son adjoint en indiquant la date et le type d'utilisation inappropriée détectée;

ii) le directeur général ou son adjoint avise l'un des gestionnaires principaux du système pour vérification et advenant que l'utilisation est identifiée inappropriée, le conseil municipal déterminera la mesure applicable.

4.8 Gestion de l'accès des visiteurs et des fournisseurs

a) Les employés et utilisateurs autorisés qui seront visités dans les bâtiments à accès sécurisés sont responsables de leurs visiteurs ou fournisseurs qui devront se soumettre aux exigences établies en vertu du contrôle des accès aux différents édifices municipaux.

b) Toutes les demandes d'autorisation d'accès aux bâtiments municipaux seront analysées par le gestionnaire de secteur.

c) Si un système de cartes, de jetons d'accès, un registre pour signature ou tout autre système de contrôle est établit pour l'accès aux édifices municipaux, les personnes visées par la présente politique devront se conformer aux exigences établies.

d) Toute personne demandant l'accès à une installation pourra faire objet de vérification pour confirmer son identité afin de réduire le risque d'entrée par une personne non autorisée.

5 SÉCURITÉ DES UTILISATEURS

5.1 Toute personne ayant accès à un bâtiment municipal avec accès sécurisé devra s'assurer que les exigences en matière de santé et sécurité soient respectées.

5.2 Le système devra en tout temps être branché à une source d'alimentation de secours permettant aux personnes à l'intérieur des bâtiments sécurisés de maintenir le système fonctionnel advenant une panne d'électricité.

6 PROCÉDURES D'ACHAT ET/OU DE REMPLACEMENT

6.1 L'achat d'équipement relié aux accès sécurisés des bâtiments municipaux doit respecter les normes et conditions exigées par la municipalité et respecter les contrats s'y rattachant, s'il y a lieu.

6.2 Tout nouveau bâtiment municipal ou rénovation majeure dans un bâtiment existant devra être considéré pour l'installation d'accès sécurisé à moins d'avis contraire émis par le conseil municipal.

7 FORMULAIRE DE CONSENTEMENT

7.1 Toute personne devant utiliser les outils d'accès sécurisé de la municipalité devra au préalable donner son consentement aux modalités de la présente politique en signant le formulaire ci-joint identifié : ANNEXE A – FORMULAIRE DE CONSENTEMENT

8 ABROGATION

8.1 Cette nouvelle politique remplace toutes les politiques, directives et guides antérieurs relatifs aux accès sécurisés des bâtiments appartenant à la municipalité d'Edmundston et à la distribution des clés.

Jacques P. Martin, Maire

Marc Michaud, DG et Secrétaire

Edmundston

ANNEXE A

FORMULAIRE DE CONSENTEMENT

POLITIQUE ADMINISTRATIVE NO. 24
ACCÈS SÉCURISÉS DES BÂTIMENTS MUNICIPAUX

Je certifie avoir reçu un exemplaire de la politique administrative N° 24 concernant les Accès sécurisés des bâtiments municipaux et je confirme l'avoir lu et en comprendre le sens. La direction a répondu de manière satisfaisante à l'ensemble de mes interrogations. Je comprends que je suis tenu de respecter la présente politique.

De plus, je comprends que la politique est de nature à évoluer. Il est donc entendu que les changements apportés peuvent entrainer le remplacement, la modification ou l'élimination de l'une ou l'autre des composantes de cette politique. Ces changements me seront communiqués au moyen d'un avis officiel. J'accepte la responsabilité de me tenir au courant de ces changements. J'affirme avoir en ma possession une copie dûment signée de la politique administrative N° 24 et que je respecterai ses exigences.

Je m'engage, dans le cadre de mes fonctions pour la municipalité d'Edmundston, d'avoir en ma possession en tout temps, la carte ou jeton d'accès qui m'a été assigné. Je suis conscient des interdictions entourant le fait de prêter ma carte ou jeton d'accès ou de l'utiliser de façon inappropriée et suis conscient des conséquences s'y rattachant.

Je m'engage à conserver ma carte ou jeton d'accès en bon état et en cas de perte, aviser le gestionnaire de secteur, dans les plus brefs délais et à assumer les frais de remplacement, s'il y a lieu. Je m'engage aussi à retourner ma carte ou jeton d'accès dans les plus brefs délais advenant mon départ définitif de l'organisation.

Nom :	
Service :	
Signature :	
Date :	