V.12.
Gestion de la sécurité physique

Vérificateur général
de la Ville de Montréal

TABLE DES MATIÈRES

1. INTRODUCTION 453

2. PORTÉE DE LA MISSION 454

3. CONSTATATIONS ET RECOMMANDATIONS 455

3.1. Gouvernance de la sécurité physique 456

3.2. Périmètre d'accès 457

3.3. Authentification et contrôle d'accès 464

3.4. Équipements de surveillance et de détection 469

3.5. Protection environnementale 472

V.12. GESTION DE LA SÉCURITÉ PHYSIQUE

1. INTRODUCTION

La Ville de Montréal (la Ville) et ses organismes contrôlés possèdent de nombreux actifs essentiels et vitaux localisés, entreposés ou détenus dans divers bâtiments, édifices et locaux. Étant donné l'importance de ces actifs, une sécurité physique adéquate doit être en place afin de protéger les édifices et les installations de la Ville contre les actes de terrorisme, de vol ou de sabotage.

La sécurité physique comprend trois niveaux de protection : le périmètre externe, le périmètre interne et l'intérieur des bâtiments, des édifices et des installations.

Le périmètre externe est défini par les limites extérieures de la propriété, mais ne se borne pas au bâtiment lui-même. En effet, il inclut, par exemple, les zones de stationnement des véhicules. Le but de sécuriser le périmètre externe est de contrôler et de permettre l'accès à la propriété uniquement aux personnes autorisées. Des moyens de contrôle divers peuvent être mis en place, allant d'une simple porte verrouillée à des guérites de sécurité avec la présence de gardiens.

Le périmètre interne comprend, entre autres, les portes, les fenêtres et les murs donnant accès à l'extérieur du bâtiment. La sécurisation du périmètre interne doit permettre d'empêcher les intrusions des personnes malintentionnées. Sa protection est réalisée par des mécanismes de sécurité tels que des serrures, des cartes d'accès et des systèmes d'alarme.

Quant au dernier niveau, l'intérieur des locaux, il nécessite également d'être protégé. Une sécurité physique adéquate des locaux permettra de contrôler et de restreindre les allées et venues des personnes, qu'il s'agisse d'employés, de contractuels ou de visiteurs. Par conséquent, des personnes non autorisées ne peuvent pas accéder à des zones sensibles telles que des salles de serveurs, des centres de communications ou des bureaux contenant des renseignements confidentiels.

Dans l'optique d'obtenir un niveau de confiance raisonnable quant à la qualité des contrôles en place pour assurer la protection physique des actifs, nous avons décidé de réaliser une mission de vérification afférente à la gestion de la sécurité physique.

2. PORTÉE DE LA MISSION

Le principal objectif de notre mission de vérification de la gestion de la sécurité physique était de fournir une évaluation indépendante de l'efficacité des contrôles mis en place pour déterminer si la sécurité physique des édifices, occupés par des employés de la Ville, est adéquate et sécuritaire.

Notre démarche de vérification a été élaborée à la suite de notre analyse de risques afférente aux édifices et au contexte de la Ville.

Nous avons défini notre démarche ainsi que nos critères de vérification selon les bonnes pratiques de l'industrie. Nous avons développé le programme de vérification en consultant plusieurs publications pertinentes.

Nous avons réalisé nos tests de vérification en présence des responsables des unités d'affaires et, le cas échéant, des responsables des sociétés de gardiennage. Nous avons procédé par entrevues auprès de ces personnes et par une visite complète des édifices.

Fondée sur les résultats de notre analyse de risques, notre vérification a porté sur un total de 17 sites couvrant sept unités d'affaires. Étant donné la nature sensible de ces sites, la liste de ceux-ci demeure confidentielle.

La vérification de la gestion de la sécurité physique portait sur les mécanismes de contrôle des aspects suivants :

- Gouvernance de la sécurité physique;
- Périmètre d'accès;
- Authentification et contrôle d'accès;

- Équipements de surveillance et de détection;
- Protection environnementale.

Les éléments suivants ont été exclus de notre vérification :

- Procédures en cas de désastre et continuité des affaires;
- Équipements de secours de type médical;
- Polices d'assurance;
- Ententes contractuelles.

3. CONSTATATIONS ET RECOMMANDATIONS

Nous présentons dans cette section les principales déficiences relevées pour l'ensemble des unités d'affaires et des sites. Pour des raisons de confidentialité, nous ne divulguons pas le détail et les résultats des tests sur la gestion de la sécurité physique. Un rapport de vérification particulier a cependant été transmis, sous le sceau de la confidentialité, aux unités d'affaires concernées qui ont validé les constatations et les recommandations qui leur étaient adressées. Ces dernières ont pris l'engagement de mettre en place les mesures correctives en conséquence.

Par ailleurs, soulignons que nous avons évalué les déficiences constatées à la lumière des niveaux d'impacts présentés dans le tableau ci-après.

Tableau 1 – Définition des niveaux d'impact

Niveau d'impact	Définition
Critique	Conséquence directe sur la sécurité ou sur la santé publique pouvant mettre en danger la santé des personnes.
Élevé	Bien qu'il y ait moins de conséquences sur la santé et la sécurité publique, en raison de la présence de nombreux actifs de grande valeur ou de renseignements hautement confidentiels et stratégiques, une intrusion nuirait de façon importante aux opérations et à la réputation de la Ville.
Modéré	En raison de la présence de certains actifs de grande valeur ou de certains renseignements confidentiels et stratégiques, une intrusion entraverait modérément les opérations de la Ville.

3.1. GOUVERNANCE DE LA SÉCURITÉ PHYSIQUE

3.1.1. ABSENCE D'ENCADREMENT DES CARTES D'ACCÈS ET DES CLÉS

3.1.1.A. Contexte et constatations

Les encadrements sont importants au sein d'une organisation afin que les différents services utilisent le même *modus operandi* en matière d'activités qui répondent aux risques d'affaires identifiés et, plus précisément dans le contexte de notre mission de vérification, qui diminuent à un niveau acceptable les risques afférents à la sécurité physique.

Par exemple, un encadrement des cartes d'accès aux édifices comprendra les exigences à respecter pour les éléments suivants :

- Demande de cartes d'accès;
- Modification des cartes d'accès;
- Révision des détenteurs des cartes d'accès;
- Suppression des cartes d'accès.

Pour 8 des 17 sites vérifiés, nous avons constaté qu'il n'existait pas d'encadrement des cartes d'accès et des clés.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Les aspects de la sécurité afférents à la gestion des cartes d'accès pourraient ne pas être tous respectés au sein des différents édifices de la Ville. Par conséquent, des personnes non autorisées pourraient avoir accès à certains locaux et commettre des actes illicites ou avoir accès à de l'information confidentielle.
- L'absence de procédure de gestion des clés pourrait avoir pour effet que des personnes non autorisées détiennent des clés et accèdent à des zones et à des locaux sensibles ou à risque.

3.1.1.B. Recommandations

Nous recommandons aux unités d'affaires concernées d'élaborer des encadrements afin de favoriser une gestion appropriée des cartes d'accès et des clés.

3.2. PÉRIMÈTRE D'ACCÈS

3.2.1. ACTIFS DE VALEUR OU CRITIQUES VISIBLES DE L'EXTÉRIEUR

3.2.1.A. Contexte et constatations

Selon les saines pratiques de l'industrie, tous les actifs de valeur ou critiques hébergés dans des locaux doivent être dérobés de la vue du public autant à l'intérieur qu'à l'extérieur des bâtiments.

Pour 2 des 17 sites vérifiés, nous avons constaté les éléments suivants :

- Les vitres extérieures d'un entrepôt contenant des actifs de valeur ne sont pas opaques, donc le public peut voir clairement ce qui se trouve à l'intérieur;
- Les vitres extérieures d'un local contenant de l'information confidentielle disposaient de rideaux, mais ces derniers n'étaient pas déployés. Par conséquent, il était possible de voir à l'intérieur et même de lire les étiquettes des boîtes les plus près des fenêtres.

Nous estimons que le **niveau d'impact est élevé,** car la Ville fait face aux risques et aux conséquences potentiels suivants : en voyant une partie du contenu de ces locaux par les fenêtres du rez-de-chaussée, une personne malintentionnée pourrait rapidement et aisément constater que ces locaux sont utilisés pour entreposer des actifs de valeur ou de l'information confidentielle. De ce fait, elle pourrait planifier des actes frauduleux (p. ex. le vol de matériel) en ciblant directement ces locaux sensibles et critiques.

3.2.1.B. Recommandations

Nous recommandons aux unités d'affaires concernées de mettre en place des mécanismes afin d'empêcher que les actifs de valeur et critiques soient visibles de l'extérieur.

3.2.2. PORTES D'ACCÈS EXTÉRIEURES AUX LOCAUX ENTROUVERTES OU NON VERROUILLÉES

3.2.2.A. Contexte et constatations

Les portes d'accès extérieures aux différents locaux des édifices sont les derniers remparts et mécanismes de protection contre les tentatives d'intrusion. Il existe deux types principaux de portes d'accès extérieures aux édifices :

- Les portes utilisées pour entrer et sortir des différents locaux des édifices. Afin de ne laisser entrer que les personnes autorisées, ce type de portes devrait être verrouillé en permanence en étant muni, par exemple, d'une serrure avec un lecteur de cartes d'accès.
- Les portes utilisées comme sorties de secours advenant une évacuation d'urgence du personnel. Selon les bonnes pratiques de l'industrie, ces portes doivent pouvoir être déverrouillées automatiquement de l'intérieur, mais elles ne doivent pas s'ouvrir de l'extérieur.

Pour 2 des 17 sites vérifiés, nous avons constaté qu'une trentaine de portes d'accès n'étaient pas verrouillées ou étaient laissées entrouvertes.

Nous estimons que le **niveau d'impact est élevé,** car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Une fois les portes d'accès franchies, les personnes non autorisées ont accès aux actifs hébergés au sein des sites et peuvent commettre des actes illicites;
- Advenant des actes frauduleux (p. ex. le vol de matériel), il serait impossible d'identifier les personnes qui sont entrées et sorties des édifices et des locaux.

3.2.2.B. Recommandations

Nous recommandons aux unités d'affaires concernées de sensibiliser leurs employés afin qu'ils ne laissent plus les portes d'accès entrouvertes ou déverrouillées.

3.2.3. ABSENCE DE CLOISONNEMENT DES ACCÈS PHYSIQUES

3.2.3.A. Contexte et constatations

Selon les bonnes pratiques de l'industrie, il est recommandé que les accès aux étages et aux locaux non destinés au public soient protégés par des mécanismes de cloisonnement des accès physiques. Ces mécanismes peuvent être, par exemple, des portes en verre installées entre les couloirs d'accès aux bureaux et la proximité des escaliers et des sorties d'ascenseurs. Ces portes sont verrouillées et disposent d'un lecteur de cartes d'accès.

Pour 1 des 17 sites vérifiés, nous avons constaté qu'une fois rendus à certains étages nous avons pu circuler librement dans les bureaux. En effet, aucun mécanisme de cloisonnement des accès physiques n'était présent.

Nous estimons que le **niveau d'impact est élevé,** car la Ville fait face aux risques et aux conséquences potentiels suivants : une personne malintentionnée pourrait réussir à emprunter les escaliers pour se rendre aux différents étages et ainsi circuler sans entrave au sein des locaux. Elle pourrait commettre des actes frauduleux ou des agressions sur des individus.

3.2.3.B. Recommandations

Nous recommandons à l'unité d'affaires concernée de mettre en place des mécanismes de cloisonnement des accès aux étages nécessaires.

3.2.4. SALLES ÉLECTRIQUES OU MÉCANIQUES NON VERROUILLÉES

3.2.4.A. Contexte et constatations

Les salles électriques et les salles mécaniques des édifices contiennent de l'équipement qui traite une grande quantité d'énergie électrique (p. ex. des transformateurs, des génératrices). Selon les saines pratiques de l'industrie, tous les locaux électriques doivent être verrouillés afin qu'ils ne soient accessibles que par les personnes autorisées, mais surtout pour éviter les accidents attribuables aux éventuelles décharges électriques.

Pour 5 des 17 sites vérifiés, nous avons constaté que les accès aux salles électriques ou mécaniques n'étaient pas verrouillés.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Une personne non autorisée qui s'introduirait dans ces locaux s'exposerait à des risques d'électrocution pouvant porter gravement atteinte à sa santé et à sa vie;
- Un sabotage ou une mise hors tension des équipements pourrait nuire à la bonne marche des activités qui ont cours dans les édifices.

3.2.4.B. Recommandations

Nous recommandons aux unités d'affaires concernées de verrouiller en permanence les accès aux salles électriques ou mécaniques afin que seules les personnes autorisées y aient accès.

3.2.5. CENTRAL TÉLÉPHONIQUE NON PROTÉGÉ

3.2.5.A. Contexte et constatations

Selon les bonnes pratiques de l'industrie, les centraux téléphoniques doivent être adéquatement protégés afin que des personnes non autorisées ne puissent pas, volontairement ou par inadvertance, endommager la multitude de câbles téléphoniques y étant localisés.

De manière générale, ces centraux téléphoniques sont situés dans une salle informatique ou réseau, ou encore dans une armoire sécuritaire si les locaux les abritant n'offrent pas une protection adéquate.

Pour 1 des 17 sites vérifiés, nous avons constaté que le central téléphonique est situé dans la salle d'entreposage des produits d'entretien et qu'il est fixé sur le mur sans aucune forme de protection.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants : en accédant au local d'entretien, une personne

non autorisée pourrait endommager les centaines de câbles sciemment ou involontairement par un mauvais geste. Par conséquent, la téléphonie pourrait éprouver des problèmes, voire devenir inopérante.

3.2.5.B. Recommandations

Nous recommandons à l'unité d'affaires concernée de protéger le central téléphonique au moyen d'une armoire de sécurité qui devra être verrouillée en permanence et uniquement accessible aux personnes autorisées.

3.2.6. PLAQUES D'IDENTIFICATION DES LOCAUX

3.2.6.A. Contexte et constatations

Les plaques d'identification du rôle des locaux sont essentiellement utilisées dans les édifices publics et privés pour diriger les visiteurs vers les salles qu'ils recherchent. Par exemple, il est commun de voir les plaques d'identification « service à la clientèle », « salle de prélèvements », « cafétéria », « accueil » et « bureau de paiements ». Toutefois, les bonnes pratiques de l'industrie recommandent que les locaux sensibles et critiques ne soient pas indiqués par des plaques ou affichettes.

Pour 3 des 17 sites vérifiés, nous avons constaté qu'environ 25 locaux sensibles et critiques étaient clairement signalés par des panneaux d'indication ou par des plaquettes apposées sur leurs portes d'accès.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants : une personne malintentionnée pourrait rapidement et aisément déterminer le rôle de certains locaux. De ce fait, elle pourrait planifier des actes frauduleux en ciblant directement les locaux sensibles et critiques.

3.2.6.B. Recommandations

Nous recommandons aux unités d'affaires concernées de retirer les plaquettes d'identification des locaux sensibles et critiques.

3.2.7. ABSENCE D'UN GARDIEN DE SÉCURITÉ

3.2.7.A. Contexte et constatations

Un gardien de sécurité permet de filtrer les visiteurs en vérifiant leur identité et en validant les motifs de leur visite. Un gardien de sécurité a également un effet dissuasif envers certaines personnes potentiellement malveillantes. Il est également formé pour pouvoir agir promptement et efficacement à l'égard des menaces.

Pour 2 des 17 sites vérifiés, nous avons constaté qu'il n'y avait aucun gardien de sécurité présent à l'accueil des édifices.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Absence d'effet dissuasif qui pourrait augmenter les possibilités de tentatives d'intrusion;
- Difficulté de faire face et d'agir efficacement en cas d'agression de la part d'un visiteur.

3.2.7.B. Recommandations

Nous recommandons aux unités d'affaires concernées de mettre en place des mesures de sécurité appropriées telles que la présence d'un gardien de sécurité.

3.2.8. RONDES DES GARDIENS DE SÉCURITÉ SANS SYSTÈME DE POINÇONS

3.2.8.A. Contexte et constatations

Le système de poinçons est utilisé par les sociétés de gardiennage afin de s'assurer que leurs gardiens de sécurité vérifient l'ensemble des éléments sensibles et critiques lorsqu'ils effectuent leurs rondes de surveillance. De plus, ce système permet de maintenir des fichiers journaux qui enregistrent le nom du gardien ainsi que la date et l'heure de passage aux points névralgiques.

Nous avons constaté qu'il n'existe pas de système de poinçons pour 3 des 17 sites vérifiés.

Nous estimons que le niveau d'impact est modéré, car sans système de poinçons, les unités d'affaires ne peuvent obtenir l'assurance que les gardiens vérifient tous les éléments et les zones sensibles et critiques au cours de leurs rondes de surveillance.

3.2.8.B. Recommandations

Nous recommandons aux unités d'affaires concernées d'exiger que les gardiens de sécurité utilisent un système de poinçons au cours de leurs rondes.

3.2.9. ABSENCE DE PROTECTION ADÉQUATE À UN POSTE DE GARDIENNAGE

3.2.9.A. Contexte et constatations

Les postes de gardiennage sont généralement situés au rez-de-chaussée des édifices près de l'entrée principale. Des gardiens y sont présents en permanence afin de contrôler les accès au site.

Selon les bonnes pratiques de l'industrie, la partie d'un poste de garde qui fait face au public devrait être munie d'un mécanisme de protection qui empêche toute tentative d'intrusion ou d'agression.

Pour 1 des 17 sites vérifiés, nous avons constaté que la partie du poste de gardiennage qui fait face au public n'est pas protégée adéquatement.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Une personne malintentionnée pourrait, à distance, atteindre les gardiens de sécurité au moyen d'un projectile (p. ex. avec une arme à feu, une arme blanche);
- Un individu pourrait s'introduire dans le poste de garde et agresser physiquement les gardiens de sécurité.

3.2.9.B. Recommandations

Nous recommandons à l'unité d'affaires concernée d'installer un mécanisme de protection sur la partie publique du poste de gardiennage afin d'éviter toute tentative d'intrusion ou d'agression.

3.2.10. SOUPIRAUX NON GRILLAGÉS

3.2.10.A. Contexte et constatations

Selon les bonnes pratiques de l'industrie, un soupirail doit être muni de mécanismes de sécurité (p. ex. une grille) afin d'empêcher les accès non autorisés.

Pour 1 des 17 sites vérifiés, nous avons constaté que trois soupiraux sur sept n'étaient pas équipés de grilles anti-intrusion.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants : des personnes malveillantes pourraient s'introduire par l'un de ces soupiraux et commettre des actes frauduleux (p. ex. un vol, du vandalisme).

3.2.10.B. Recommandations

Nous recommandons à l'unité d'affaires concernée d'installer des grilles anti-intrusion sur les trois soupiraux de l'édifice en question.

3.3. AUTHENTIFICATION ET CONTRÔLE D'ACCÈS

3.3.1. ABSENCE DE PROCESSUS DE RÉVISION DES DÉTENTEURS DE CLÉS ET DE CARTES D'ACCÈS

3.3.1.A. Contexte et constatations

De nombreuses clés et cartes d'accès sont utilisées pour sécuriser différents locaux des édifices. Il est très important qu'un processus de révision périodique des détenteurs de clés et de cartes d'accès soit mis en place afin de s'assurer que seules les personnes autorisées en possèdent. En effet, ce processus de révision permet :

- de faire l'inventaire exhaustif des clés et des cartes d'accès;
- de déterminer quelles sont les clés ou cartes d'accès qui ont été perdues ou volées et de prendre les actions nécessaires pour changer ou modifier les serrures en cause ou désactiver les cartes d'accès;

- de reprendre les clés et les cartes d'accès détenues par des personnes dont les rôles et responsabilités ne justifient pas ou plus qu'elles soient en possession de celles-ci.

Pour 11 des 17 sites vérifiés, nous avons constaté qu'il n'y a aucun processus de révision des détenteurs de clés et de cartes d'accès.

Nous estimons que le **niveau d'impact est élevé,** car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Impossibilité de savoir avec exactitude quelles sont les clés en circulation et par qui elles sont détenues;
- Des personnes non autorisées pourraient accéder aux locaux et effectuer des actes illicites tels que du sabotage, du vol de matériel ou de renseignements confidentiels.

3.3.1.B. Recommandations

Nous recommandons aux unités d'affaires concernées :

- **de mettre en place un processus récurrent de révision des détenteurs de clés et de cartes d'accès;**
- **de remplacer ou de modifier les serrures pour lesquelles les clés ont été perdues ou volées en tenant compte du risque encouru;**
- **de reprendre les clés et les cartes d'accès des personnes dont les rôles et responsabilités ne requièrent plus la détention de celles-ci;**
- **de maintenir à jour l'inventaire des clés et des cartes d'accès.**

3.3.2. DROITS D'ACCÈS NON JUSTIFIÉS À CERTAINS LOCAUX SENSIBLES

3.3.2.A. Contexte et constatations

Les accès aux différents édifices et locaux sont protégés par des lecteurs de cartes d'accès. Un tel système permet de gérer les droits d'accès du personnel de manière très précise afin d'octroyer les accès uniquement aux personnes autorisées.

Pour 3 des 17 sites vérifiés, nous avons constaté que des droits d'accès avaient été attribués à des individus sans que ce soit exigé par leurs rôles et responsabilités, et certains de ces droits donnaient accès à des locaux sensibles.

Nous estimons que le **niveau d'impact est élevé,** car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Accès aux locaux et aux actifs par des personnes non autorisées;
- Indisponibilité des actifs et perte de confidentialité des données.

3.3.2.B. Recommandations

Nous recommandons aux unités d'affaires concernées de supprimer les droits d'accès non justifiés, de par leurs rôles et responsabilités, des détenteurs de cartes d'accès.

3.3.3. PRÉSENCE DE DOUBLONS DANS UN DES SYSTÈMES DE GESTION DE CARTES D'ACCÈS

3.3.3.A. Contexte et constatations

Un système de gestion de cartes d'accès est utilisé pour gérer les accès physiques aux édifices et aux locaux de la Ville.

Pour 5 des 17 sites vérifiés, nous avons constaté qu'il y avait des comptes en double pour plusieurs employés au sein du système de gestion des cartes d'accès. En effet, ces employés disposaient de deux comptes avec des droits d'accès identiques ou concurrents.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants : advenant une modification ou une suppression d'accès, il se pourrait que seul un des deux comptes d'employé soit mis à jour. Par conséquent, l'employé conserverait des droits d'accès qui ne sont plus justifiés.

3.3.3.B. Recommandations

Nous recommandons à l'unité d'affaires concernée de supprimer les doublons de détenteurs de cartes d'accès.

3.3.4. SALLES INFORMATIQUES ET RÉSEAU NON MUNIES D'UN LECTEUR DE CARTES D'ACCÈS

3.3.4.A. Contexte et constatations

Selon les bonnes pratiques de l'industrie et afin de pouvoir contrôler quelles sont les personnes qui accèdent aux salles informatiques et de télécommunications, les portes de celles-ci doivent être munies d'un système de verrouillage avec un lecteur de cartes d'accès. Ce type de lecteur permet de disposer de fichiers journaux qui enregistrent, de manière chronologique, les détenteurs de cartes qui entrent et sortent des locaux informatiques. Advenant des événements tels que le vol de matériel, il serait aisé d'identifier quelles ont été les personnes qui étaient présentes sur les lieux au moment des faits et, par conséquent, de déterminer qui est l'auteur du vol.

Pour 3 des 17 sites vérifiés, nous avons constaté que les salles informatiques ou réseau n'étaient pas munies d'un lecteur de cartes d'accès.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Impossibilité de déterminer et d'identifier quelles ont été les personnes présentes en cas d'actes frauduleux (p. ex. une dégradation du matériel, un vol);
- Une personne non autorisée pourrait accéder aux salles et aux équipements réseau et installer du matériel permettant de capter les données qui transitent sur le réseau des édifices;
- Perte de disponibilité, d'intégrité et de confidentialité des données traitées et hébergées par les serveurs et les équipements réseau.

3.3.4.B. Recommandations

Nous recommandons aux unités d'affaires concernées d'installer des serrures avec un lecteur de cartes d'accès sur les portes des salles informatiques et réseau.

3.3.5. LECTEURS DE CARTES D'ACCÈS NON FONCTIONNELS

3.3.5.A. Contexte et constatations

Tel que nous l'avons décrit dans les précédentes sections, les lecteurs de cartes d'accès permettent une gestion sécuritaire des accès aux édifices. Si ces derniers ne fonctionnent pas, il faut alors recourir aux clés et il sera impossible de contrôler efficacement les entrées et sorties des personnes.

Pour 1 des 17 sites vérifiés, nous avons constaté que sept lecteurs de cartes d'accès n'étaient pas fonctionnels. Il est à mentionner que toutes les portes d'accès étaient verrouillées au moment de notre visite.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants : impossibilité de déterminer et d'identifier quelles ont été les personnes qui sont entrées et sorties des locaux advenant la perpétration d'actes frauduleux (p. ex. une dégradation du matériel, un vol).

3.3.5.B. Recommandations

Nous recommandons à l'unité d'affaires concernée de mettre en état de fonctionnement les sept lecteurs de cartes d'accès.

3.3.6. SERRURES À CODE

3.3.6.A. Contexte et constatations

Avant l'avènement des systèmes de contrôle d'accès par cartes, les serrures à code étaient utilisées afin de contrôler les accès aux zones sensibles et critiques. Une serrure ne pouvant avoir plus d'un code d'accès, celui-ci était diffusé à plusieurs personnes autorisées. Cependant, il était impossible d'identifier et de déterminer

précisément qui accédait aux locaux et à quel moment précis. Ce système de serrures donne la possibilité de changer le code régulièrement. Mais, en règle générale, cette fonction est rarement appliquée.

Pour 3 des 17 sites vérifiés, nous avons constaté que plusieurs portes intérieures étaient munies d'une serrure à code. De plus, certains codes n'ont pas été changés depuis une quinzaine d'années.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Bien que les serrures à code soient plus sécuritaires que les serrures traditionnelles, elles ne permettent pas de s'assurer que seules les personnes autorisées ont accès à ces locaux. En effet, les codes n'étant pas changés régulièrement, ils deviennent connus de nombreuses personnes n'ayant pas besoin de tels accès dans le cadre de leurs fonctions.
- Advenant des événements frauduleux (p. ex. un vol de matériel, un vol de renseignements stratégiques), il ne serait pas possible de déterminer qui était présent sur les lieux au moment des faits.

3.3.6.B. Recommandations

Nous recommandons aux unités d'affaires concernées de remplacer les serrures à code par des lecteurs de cartes d'accès.

3.4. ÉQUIPEMENTS DE SURVEILLANCE ET DE DÉTECTION

3.4.1. CAMÉRAS DE VIDÉOSURVEILLANCE DÉFECTUEUSES OU NE COUVRANT PAS L'ENSEMBLE DES ZONES SENSIBLES ET SYSTÈME ANALOGIQUE

3.4.1.A. Contexte et constatations

Un système de caméras de vidéosurveillance est composé de plusieurs caméras disposées à des endroits stratégiques du périmètre externe et interne d'un édifice afin d'enregistrer les personnes qui empruntent les différents points d'entrée et de sortie.

Les images provenant de ces caméras sont enregistrées et archivées de manière numérique sur des supports électroniques tels que des DVD ou des disques durs.

Un tel système permet, entre autres, de dissuader les personnes malintentionnées de commettre un délit, de retrouver et d'identifier facilement les personnes liées à un événement, et de vérifier les fausses alarmes.

CAMÉRAS DÉFECTUEUSES ET NE COUVRANT PAS L'ENSEMBLE DES ZONES SENSIBLES

Au cours de nos travaux de vérification, nous avons constaté les lacunes suivantes :

- Pour 1 des 17 sites vérifiés, 72 % des caméras de vidéosurveillance n'étaient pas fonctionnelles;
- Pour 1 des 17 sites vérifiés, deux angles morts ne permettaient pas aux caméras de vidéosurveillance d'enregistrer les événements de ces deux zones sensibles;
- Pour 5 des 17 sites vérifiés, l'ensemble des zones sensibles n'était pas surveillé par des caméras de sécurité.

Nous estimons que le **niveau d'impact est élevé.** Avec un tel nombre de caméras non fonctionnelles ou manquantes, la Ville fait face aux risques et aux conséquences potentiels suivants :

- La surveillance du périmètre externe et des entrées et sorties des visiteurs ne peut pas être effectuée de manière à couvrir tous les points d'accès sensibles aux sites et aux différents édifices et locaux;
- En cas d'incidents, il serait difficile, voire impossible, d'identifier les auteurs d'actions frauduleuses.

SYSTÈME DE VIDÉOSURVEILLANCE ANALOGIQUE

Pour 2 des 17 sites vérifiés, nous avons constaté que les images provenant des caméras du système de vidéosurveillance étaient enregistrées sur des cassettes VHS qui sont des supports désuets.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants :

- Difficulté croissante d'approvisionnement en support d'enregistrement VHS;
- Coûts des supports d'enregistrement VHS et de leur archivage plus élevés que les supports numériques (p. ex. DVD, disques durs);
- Difficulté de faire des recherches et d'identifier les individus en cas d'actes illicites. En effet, la qualité des images VHS, donc analogiques, est très en deçà de la qualité des enregistrements numériques.

3.4.1.B. Recommandations

Nous recommandons aux unités d'affaires concernées :

- **de remettre en état de fonctionnement les caméras de vidéosurveillance défectueuses et de s'assurer que toutes les caméras restent opérationnelles;**
- **de déplacer les caméras afin qu'il n'y ait plus d'angle mort;**
- **d'installer des caméras de surveillance afin de couvrir l'ensemble des zones sensibles et critiques.**

Nous recommandons également aux unités d'affaires concernées de remplacer leur système d'enregistrement de vidéosurveillance analogique par un système d'enregistrement numérique.

3.4.2. SYSTÈMES D'ALARME ANTI-INTRUSION ABSENTS OU NON BRANCHÉS

3.4.2.A. Contexte et constatations

Les systèmes d'alarme anti-intrusion sont installés, entre autres, sur les clôtures, sur les portes et sur les fenêtres d'un édifice pouvant être atteintes relativement facilement par une personne de l'extérieur.

Aussitôt qu'une clôture, une porte ou une fenêtre sous alarme est ouverte, forcée ou brisée, un signal est immédiatement envoyé à une centrale de surveillance pour avertir les gardiens de sécurité qu'un incident anormal est en cours. Ils peuvent alors agir promptement pour vérifier si l'alarme est justifiée et ainsi mettre fin aux éventuelles tentatives d'intrusion physique.

Pour 2 des 17 sites vérifiés, nous avons constaté qu'aucun système d'alarme anti-intrusion n'était installé.

Pour 2 des 17 sites vérifiés, nous avons constaté qu'un système d'alarme anti-intrusion était installé, mais n'était pas branché.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants : des personnes malveillantes pourraient s'introduire dans les locaux. Le site n'étant pas sous alarme, les gardiens de sécurité du poste de surveillance ne seraient pas avisés qu'une tentative d'intrusion est en cours. Par conséquent, les délais d'intervention des gardiens ne leur permettraient pas d'empêcher, en temps opportun, la perpétration d'actes frauduleux.

3.4.2.B. Recommandations

Nous recommandons aux unités d'affaires concernées :

- **d'étudier la possibilité d'installer un système d'alarme anti-intrusion afin de protéger leurs actifs de valeur;**
- **de rendre fonctionnels les deux systèmes d'alarme installés mais non branchés.**

3.5. PROTECTION ENVIRONNEMENTALE

3.5.1. ABSENCE DE DÉTECTEUR D'INCENDIE DANS UNE SALLE INFORMATIQUE

3.5.1.A. Contexte et constatations

Les détecteurs d'incendie et de fumée dans les salles informatiques permettent de déceler et d'aviser sans tarder les équipes d'intervention en cas de début d'incendie. Par conséquent, l'incendie peut être circonscrit avant que les serveurs, les équipements réseau et les données soient détruits.

Pour 1 des 17 sites vérifiés, nous avons constaté qu'une salle informatique n'était pas munie de détecteur de fumée et d'incendie.

Nous estimons que le niveau d'impact est modéré, car la Ville fait face aux risques et aux conséquences potentiels suivants : intervention tardive pouvant mener à la destruction des serveurs, des données et des équipements réseau hébergés dans la salle informatique.

3.5.1.B. Recommandations

Nous recommandons à l'unité d'affaires concernée d'installer un système de détection des incendies dans la salle informatique.