V.12.
Physical Security Management

Vérificateur général
de la Ville de Montréal

TABLE OF CONTENTS

1. INTRODUCTION 413

2. AUDIT SCOPE 414

3. FINDINGS AND RECOMMENDATIONS 415

3.1. Physical Security Governance 415

3.2. Access Perimeter 416

3.3. Identity Authentication and Access Control 423

3.4. Surveillance and Detection Equipment 428

3.5. Environmental Protection 431

V.12. PHYSICAL SECURITY MANAGEMENT

1. INTRODUCTION

The Ville de Montréal (the city) and the bodies it controls own a number of important, valuable assets located, stored or kept in various municipal buildings and facilities. Given how important these items are, adequate physical security measures must be put into place to protect these buildings and facilities against acts of terrorism, theft and sabotage.

Physical security comprises three levels of protection: outer perimeter, inner perimeter and building interior.

The outer perimeter refers to the outside limits of a property, excluding the actual building. It can include such areas as parking lots. The goal in securing the outer perimeter is to control access and make sure that only authorized individuals enter a property. Various approaches can be taken in this regard, from a simple lock on a gate to a fully staffed security checkpoint.

The inner perimeter refers to such things as doors, windows and walls through which an individual can enter a building. Securing the inner perimeter involves preventing intruders from entering the building interior. This is achieved through such security devices as door locks, access cards and alarm systems.

The last level of physical security—the building interior—also needs to be protected. Adequate interior security makes it possible to control the comings and goings of employees, consultants, visitors and others and ensure that unauthorized individuals do not have access to sensitive areas, such as server rooms, communications centres and offices where confidential information is kept.

To be reasonably assured of the quality of the physical controls in place to protect the city's assets, we decided to assess physical security management during our audit.

2. AUDIT SCOPE

The main purpose of our audit of physical security management was to provide an independent review of the effectiveness of the controls that have been put in place and thus determine whether the physical security of buildings occupied by city employees is appropriate and adequate.

Our approach was developed following our risk analysis of city buildings and their context.

We based our approach and our audit criteria on industry best practices and developed our audit program after consulting several relevant publications.

We performed our audit tests in the presence of officials from the relevant business units and, when applicable, representatives of the security companies used by the city. We interviewed these individuals and took a comprehensive tour of the audited facilities.

Following our risk analysis, we focused our audit on a total of 17 sites involving seven business units. Given their sensitive nature, the list of these sites will remain confidential.

The physical security management audit concentrated on controls related to:

- physical security governance
- access perimeter
- access authentication and control
- surveillance and detection equipment
- environmental protection

The following elements were excluded from our audit:

- disaster management and business continuity procedures
- emergency equipment of a medical nature
- insurance policies
- contractual agreements

3. FINDINGS AND RECOMMENDATIONS

In this section, we will outline the main deficiencies observed in the various business units and sites we audited. For confidentiality purposes, we will not disclose the details and results of the physical security management tests that we conducted. A special audit report was nevertheless submitted confidentially to the relevant business units, which corroborated the findings and recommendations pertaining specifically to them. Each of the units has committed to putting the corrective measures in place.

We assessed the observed deficiencies based on three impact levels, as indicated in Table 1.

Table 1—Description of Impact Levels

Level of impact	Definition
Critical	Direct consequence on public safety or health that may endanger the health of individuals.
High	Although there is less of a threat to public health or safety at this level, the presence of many high-value assets or highly confidential and strategic information implies that an intrusion would severely damage the city's operations and reputation.
Moderate	Given the presence of some high-value assets or certain confidential or strategic information, an intrusion would interfere moderately with the city's operations.

3.1. PHYSICAL SECURITY GOVERNANCE

3.1.1. UNMONITORED USE OF ACCESS CARDS AND KEYS

3.1.1.A. Background and Findings

It is important to adopt a structured system in an organization to ensure that the various departments operate the same way in response to identified business risks. In the context of this particular audit, a structured system would help reduce physical security–related risk to an acceptable level.

For example, a well-structured building access card system would include requirements related to several factors:

- requests for access cards
- changes in access cards
- review of cardholders
- deactivation of access cards

Eight of the 17 sites we audited had no structured system in place to control access cards and keys.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences:

- Security considerations related to access card management may not be followed fully in every municipal building. As a result, unauthorized individuals may gain access to premises where they can commit unlawful acts or access confidential information.
- Given the lack of management procedures for controlling the use of keys, it is possible that unauthorized individuals have possession of keys that let them enter sensitive or high-risk areas or premises.

3.1.1.B. Recommendations

We recommend that the relevant business units develop a structured system to help ensure the appropriate management of access cards and keys.

3.2. Access Perimeter

3.2.1. Valuable or Critical Assets Visible from the Outside

3.2.1.A. Background and Findings

In accordance with industry best practices, all valuable or critical assets found within a building must be hidden from public view, both from the inside and from the outside.

In 2 of the 17 sites we audited, however, we noted that:

- The exterior windows of a warehouse where valuable assets were being stored were not opaque. The public could therefore clearly see the contents from the outside.
- The exterior windows of a room containing confidential information were fitted with curtains, but these curtains were not shut. As a result, it was possible to see the contents of the room from the outside and even read the labels on the boxes closest to the windows.

In our opinion, the **impact level of this situation is high,** exposing the city to the following risks and potential consequences: ill-intentioned individuals seeing some of the contents in these rooms through a ground-floor window could quickly and easily deduce that there are valuable assets or confidential information on the premises. Based on these observations, they could make plans to commit theft or perpetrate other acts that target these sensitive or critical areas.

3.2.1.B. Recommendations

We recommend that the relevant business units undertake measures to prevent valuable or critical assets from being visible from the outside.

3.2.2. Exterior Doors Left Unlocked or Ajar

3.2.2.A. Background and Findings

A building’s exterior doors are the last line of defence and protection against intrusion from an outside source. There are two main types of exterior doors:

- Doors that are used to go in and out of various parts of a building. These types of doors should be equipped with locking mechanisms, such as an access card reader, and kept locked at all times to prevent unauthorized individuals from entering the premises.
- Doors that are used as emergency exits during an evacuation. Although best industry practices dictate that these doors allow egress to the outside at all times, at the same time they must not allow entry to the interior.

In 2 of the 17 sites we audited, some 30 exterior doors were unlocked or ajar.

In our opinion, the **impact level of this situation is high,** exposing the city to the following risks and potential consequences:

- Unauthorized individuals who enter a building through an unlocked door will be gaining access to the assets found on the premises and may use this access for illicit purposes.
- Should theft or other illegal acts be committed, it would be impossible to determine who had been on the premises at the time.

3.2.2.B. Recommendations

We recommend that the relevant business units impress upon their employees the importance of not leaving doors unlocked or ajar.

3.2.3. No Partitions to Prevent Physical Access

3.2.3.A. Background and Findings

According to best industry practices, floors and rooms that are not intended for public use should be closed off and protected by some form of access control mechanism. These mechanisms include glass partitions and doors installed in the hallways running between offices or near staircases and elevators. These glass doors should be equipped with an access-card reader and kept locked at all times.

In 1 of the 17 sites we audited, we found that, once we were on certain floors, we had unrestricted access to offices, as there were no access control mechanisms in place whatsoever.

In our opinion, the **impact level of this situation is high,** exposing the city to the following risks and potential consequences: ill-intentioned individuals could access various floors via the staircases and walk around the premises unhindered, free to commit illegal actions or cause harm to building occupants.

3.2.3.B. Recommendations

We recommend that the relevant business unit install partitions near staircases and elevator doors to control access to the floors where required.

3.2.4. Unlocked Electrical and Mechanical Rooms

3.2.4.A. Background and Findings

Electrical and mechanical rooms contain transformers, generators and other high-voltage equipment. Industry best practices dictate that all electrical rooms be locked to restrict access to authorized individuals and, specifically, to avoid accidents due to electrical discharge.

In 5 of the 17 sites we audited, electrical or mechanical rooms were not locked.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences:

- Unauthorized individuals who enter an electrical or mechanical room would be exposed to the risk of electrocution and severe, life-threatening injury.
- If the electrical equipment were to be sabotaged or shut down, it could disrupt building operations.

3.2.4.B. Recommendations

We recommend that the relevant business units ensure that electrical and mechanical rooms remain locked at all times and that only authorized individuals have access to these facilities.

3.2.5. Unprotected Telecommunications Equipment

3.2.5.A. Background and Findings

According to industry best practices, telecommunications equipment must be sufficiently protected to prevent unauthorized individuals from accidentally or deliberately damaging the many wires and cables found there.

Generally speaking, telecommunications equipment is housed in an IT or network room or in a secure cabinet if the surrounding facilities do not offer adequate protection.

In 1 of the 17 sites we audited, the telecommunications equipment was located in a maintenance storage room. It was affixed to a wall and devoid of any form of protection.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences: unauthorized individuals could advertently or inadvertently damage hundreds of cables, thereby interfering with or even completely disrupting telecommunications services.

3.2.5.B. Recommendations

We recommend that the relevant business unit ensure that telecommunications equipment is housed in a secure cabinet that remains locked at all times and is accessible only to authorized individuals.

3.2.6. ROOM IDENTIFICATION SIGNS

3.2.6.A. Background and Findings

The main goal of room identification signs in a public or private building is to help visitors find where they are going. Common signs might read something like “Customer Service,” “Samples Room,” “Cafeteria,” “Reception” and “Payments.” Industry best practices specify, however, that facilities of a sensitive or critical nature should not bear identifying signage.

In 3 of the 17 sites we audited, some 25 sensitive or critical areas were clearly identified with information signs or nameplates on the door.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences: ill-intentioned individuals could quickly and easily determine the purpose of certain rooms and, based on these observations, make plans to commit theft or perpetrate other acts that target these sensitive or critical areas.

3.2.6.B. Recommendations

We recommend that the relevant business units remove identification signs from all rooms where sensitive or critical operations are located.

3.2.7. LACK OF SECURITY GUARDS

3.2.7.A. Background and Findings

Security guards screen incoming visitors by checking their identity and verifying the reason for their visit. The very presence of security guards can also help deter potential intruders. Moreover, security guards are trained to respond swiftly and decisively to threats.

In 2 of the 17 sites we audited, there were no security guards in the building lobby.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences:

- Lack of this deterrent could increase the likelihood of attempted intrusions.
- Without a security guard, it is difficult to ensure an effective response should a visitor become aggressive.

3.2.7.B. Recommendations

We recommend that the relevant business units implement the appropriate security measures, including the use of an on-site security guard.

3.2.8. LACK OF SECURITY PATROL REPORTING SYSTEM

3.2.8.A. Background and Findings

A reporting system is used by security companies to ensure guards check all sensitive and critical areas during their routine patrols. The system includes security logs that record the name of the security guard on duty, as well as the date and time key areas are checked.

In 3 of the 17 sites we audited, a security reporting system was not being used.

In our opinion, the impact level of this situation is moderate. Without a reporting system in place, business units cannot be assured that security guards are checking all of the required elements and sensitive and critical areas during their routine patrols.

3.2.8.B. Recommendations

We recommend that the relevant business units require security companies to use a reporting system during guards' routine patrols.

3.2.9. UNPROTECTED SECURITY GUARD STATION

3.2.9.A. Background and Findings

Security guard stations are generally located on the ground floor of a building, near the main entrance. Security guards are permanently stationed there to control access to the premises.

Based on industry best practices, the portion of the security guard station that is accessible by the public should be equipped with a structure that protects against acts of intrusion or aggression.

In 1 of the 17 sites we audited, the portion of the security guard station that is accessible by the public was not adequately protected.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences:

- Security guards are vulnerable to attack via a projectile or other weapon (e.g., a firearm or a knife).
- Anybody could enter the security guard station and physically assault the guards.

3.2.9.B. Recommendations

We recommend that the relevant business unit install a protective structure around the portion of the security guard station that is accessible by the public to deter potential intruders and attackers.

3.2.10. Unprotected Basement Windows

3.2.10.A. Background and Findings

According to industry best practices, basement windows should be fitted with protective grilles or other security devices to prevent unauthorized access.

In 1 of the 17 sites we audited, three of the seven basement windows were not equipped with security grilles.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences: intruders could enter the building via these windows and commit vandalism or other criminal acts.

3.2.10.B. Recommendations

We recommend that the relevant business unit install security grilles on the three unprotected basement windows.

3.3. Identity Authentication and Access Control

3.3.1. Lack of a Keyholder/Cardholder Review Process

3.3.1.A. Background and Findings

Numerous keys and access cards are used to secure areas in municipal buildings. It is very important that the list of keyholders and cardholders be reviewed on a regular basis to ensure that only authorized individuals have access to locked facilities. A review process makes it possible to:

- develop an exhaustive inventory of keys and access cards
- determine which keys and access cards have been lost or stolen and take the necessary action to change or reprogram the affected locks or access cards
- recover keys and access cards from individuals whose roles and responsibilities do not justify or no longer justify their having them

In 11 of the 17 sites we audited, there was no keyholder/cardholder review process in place.

In our opinion, the **impact level of this situation is high,** exposing the city to the following risks and potential consequences:

- inability to establish an accurate list of the keys in circulation and the names of the people to whom they have been issued
- ability of unauthorized individuals to access restricted premises and sabotage the facilities, steal material or confidential information or commit other criminal acts

3.3.1.B. Recommendations

We recommend that the relevant business units:

- **implement an ongoing keyholder/cardholder review process**
- **replace or modify locks for which keys have been lost or stolen, depending on the level of risk involved**
- **recover keys and access cards from those individuals whose roles and responsibilities no longer require them to access the corresponding restricted areas**
- **keep an up-to-date inventory of all keys and access cards**

3.3.2. UNJUSTIFIED ACCESS RIGHTS TO CERTAIN SENSITIVE PREMISES

3.3.2.A. Background and Findings

Access to various municipal buildings and premises is controlled by access card readers. This system makes it possible to manage access rights with a high degree of accuracy and ensure these rights are granted solely to authorized personnel.

In 3 of the 17 sites we audited, access rights had been granted to individuals whose roles and responsibilities did not justify it. In some cases, this included access to sensitive premises.

In our opinion, the **impact level of this situation is high,** exposing the city to the following risks and potential consequences:

- access by unauthorized individuals to restricted premises and assets
- unavailability of assets and breach of data confidentiality

3.3.2.B. Recommendations

We recommend that the relevant business units deactivate unjustified access rights for those cardholders whose roles and responsibilities no longer require them to be so entitled.

3.3.3. Duplicate Entries in Access Card Management System

3.3.3.A. Background and Findings

An access card management system is used to control physical access to municipal buildings and premises.

In 5 of the 17 sites we audited, a number of employees were recorded in the access card management system twice. These employees had been assigned two user accounts for which the access rights were identical or conflicting.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences: in the event an employee’s access rights are modified or revoked, these changes might be made in one of the accounts but not the other. As a result, the employee would retain rights to which he or she was no longer entitled.

3.3.3.B. Recommendations

We recommend that the relevant business unit delete duplicate cardholder records.

3.3.4. IT AND NETWORK ROOMS WITHOUT ACCESS CARD READERS

3.3.4.A. Background and Findings

In accordance with industry best practices, and to control access to IT and telecommunications rooms, the doors to these facilities must be equipped with locking systems and access card readers. The system makes it possible to use cardholder information to keep a chronological log of incoming and outgoing IT room users. In the event of a theft or other incident, this information would help determine who was in the area at the time and identify the perpetrator.

In 3 of the 17 sites we audited, the IT or network rooms were not equipped with an access card reader.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences:

- inability to identify individuals present during an act of sabotage, theft or other wrongdoing
- ability of an unauthorized individual to gain access to network rooms and equipment and install a device to hack into the building's system and steal data
- loss of availability, integrity and confidentiality of the data processed by and stored on network servers and facilities

3.3.4.B. Recommendations

We recommend that the relevant business units install locks and access card readers on all IT and network room doors.

3.3.5. DEFECTIVE ACCESS CARD READERS

3.3.5.A. Background and Findings

As we indicated earlier, access card readers make it possible to ensure that access to municipal buildings is secure. If these readers are out of order, the city has to resort to using keys, which makes it impossible to effectively monitor the comings and goings of occupants and visitors.

In 1 of the 17 sites we audited, seven access card readers were defective. It is important to note, however, that the doors in question were still locked.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences: inability to identify individuals who have entered and exited the premises, in the event of sabotage, theft or other criminal acts.

3.3.5.B. Recommendations

We recommend that the relevant business unit ensure the defective access card readers are operating properly.

3.3.6. CODE-OPERATED LOCKS

3.3.6.A. Background and Findings

Before the advent of access card systems, code-operated locks were used to control access to sensitive and critical areas. Each lock was programmed with a single access code, and this same code was provided to several authorized individuals. This system could not be used, however, to accurately identify who was on the premises and when. Although the code could be reprogrammed regularly, this was not a routine practice in most cases.

In 3 of the 17 sites we audited, several inside doors were equipped with code-operated locks. Some of these codes had remained the same for roughly 15 years.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences:

- Although code-operated locks are more secure than traditional key-operated locks, they cannot ensure that access to a given area will be restricted exclusively to authorized individuals. Because the codes are not changed on a regular basis, they are known to numerous individuals who do not need access to these premises to fulfill their duties.

- If material or strategic information is stolen or another act of wrongdoing is committed, it would not be possible to determine who was on the premises at the time.

3.3.6.B. Recommendations

We recommend that the relevant business units replace code-operating locks with access card systems.

3.4. Surveillance and Detection Equipment

3.4.1. Defective, Poorly Positioned and Outdated Surveillance Cameras

3.4.1.A. Background and Findings

A surveillance camera system consists of several cameras strategically located along the outside and inside perimeters of a building to monitor individuals at entry and exit points. The images captured by these cameras are recorded and archived digitally using electronic media such as DVDs or hard drives.

The main goals of a surveillance camera system are to act as a deterrent to potential perpetrators, easily identify the individuals involved in incidents and check for false alarms.

Defective Cameras and Cameras Not Properly Positioned to Cover Sensitive Areas

During our audit, we noted the following problems:

- In 1 of the 17 sites we audited, 72% of surveillance cameras were non-operational.
- In 1 of the 17 sites we audited, two blind spots prevented the surveillance cameras from recording incidents that occurred in two sensitive areas.
- In 5 of the 17 sites we audited, none of the sensitive areas were being monitored by surveillance cameras.

In our opinion, the **impact level of this situation is high**, exposing the city to the following risks and potential consequences:

- Outside-perimeter surveillance of incoming and outgoing visitors cannot be conducted in a way that covers all the sensitive access points on site and within the different buildings and rooms.
- Should an incident occur, it would be difficult, even impossible, to identify the perpetrators.

ANALOG VIDEO SURVEILLANCE SYSTEM

In 2 of the 17 sites we audited, the video surveillance system feed was being recorded on VHS cassettes, an outdated technology.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences:

- growing difficulty in finding VHS tapes for recording video feeds
- cost of VHS recording and archiving is higher than digital media solutions (DVDs, hard disk, etc.)
- difficulty in searching through recorded footage and identifying perpetrators, given the much lower image quality of analog VHS images compared with digital recordings

3.4.1.B. Recommendations

We recommend that the relevant business units:

- **repair defective surveillance cameras and ensure all cameras remain operational**
- **adjust camera positioning to avoid blind spots**
- **install surveillance cameras in a way that ensures that all sensitive and critical areas are covered**

We also recommend that the relevant business units upgrade their video surveillance recording systems from analog to digital.

3.4.2. ABSENT OR DISCONNECTED INTRUSION ALARM SYSTEMS

3.4.2.A. Background and Findings

Intrusion alarm systems are installed at a number of points, including fences, doors and windows that are relatively easy to access from the outside.

If a gate, door or window is opened, tampered with or broken, an alarm is immediately sent to a surveillance centre to alert security guards. This enables them to take swift action to check whether the alarm is genuine and, if so, to try to thwart the attempted intrusion.

Two of the 17 sites we audited were not equipped with an intrusion alarm system.

In 2 of the 17 sites we audited, an intrusion alarm system was installed but was not connected.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences: ill-intentioned individuals could access the premises and, because the property is not equipped with an alarm system, they could do so without the system alerting the security guards that an intrusion was in progress. Consequently, the guards would not be able to take timely action to deal with the perpetrators.

3.4.2.B. Recommendations

We recommend that the relevant business units:

- **look into the possibility of installing intrusion alarm systems to protect their valuable assets**
- **connect the two alarm systems that are already installed but not operational**

3.5. Environmental Protection

3.5.1. Lack of Fire Detectors in IT Rooms

3.5.1.A. Background and Findings

Fire and smoke detectors installed in IT rooms make it possible to identify problems and immediately advise fire response teams of an incident. This helps contain a fire before servers, network equipment and data are destroyed.

In 1 of the 17 sites we audited, one IT room was not equipped with a smoke and fire detector.

In our opinion, the impact level of this situation is moderate, exposing the city to the following risks and potential consequences: slower response time, which could result in the destruction of servers, data and network equipment in the IT room.

3.5.1.B. Recommendations

We recommend that the relevant business unit install a fire detection system in the IT room.