Access Management Guide

GCPSG-006 (2024)

Prepared By:
Royal Canadian Mounted Police
Lead Security Agency for Physical Security
Departmental Security
NHQ 73 Leikin Drive Ottawa Ontario, K1A 0R2

Publication Issued: 2024-01-15
Updated:

Foreword

The Access Management Guide is an UNCLASSIFIED publication, issued under the authority of the Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

This is a Government of Canada publication to serve as a guide for the design and management of access management systems for departments, agencies, and employees of the Government of Canada.

Suggestions for amendments and other information can be sent to the RCMP Lead Security Agency RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Effective Date

The effective date of GCPSC-006 Access Management Guide is 2024-01-15

Record of Amendments

Amendment No.	Date	Entered By	Summary of Amendment

Note: Authority for modifications or variances is Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

Contents

1. Introduction

The RCMP, as the Lead Security Agency (LSA) for physical security for the Government of Canada (GC) is responsible for providing advice and guidance on all matters relating to physical security.

1.1. Purpose

The purpose of this guide is to provide GC employees with guidance on baseline physical security access management concepts. For detailed information, GC employees should refer to their departmental security policies, standards and guidelines, the Policy on Government Security (PGS), Appendix C of the Directive on Security Management (DSM) and other RCMP LSA Guides to implement the appropriate measures to counter threats to GC employees, information, assets, and service delivery and to provide consistent safeguarding for the GC.

The guide contains both required security control safeguards, indicated by use of the word "must" and recommended security control safeguards or guidance, indicated by the use of the word "should". Use of the word "must" indicates a reference to an established GC policy or standard while the use of the word "should", refers to advice guidance or a best practice.

Baseline physical security measures are designed to provide protection against common types of threats that GC departments and agencies may encounter. Certain departments and agencies or operational activities may face different threats because of the nature of their business, their location or the attractiveness of their assets. Examples include police or military establishments, health services, laboratories, sensitive research facilities, museums, service counters, offices in high-crime areas and facilities located outside of Canada.

1.2. Applicability, Roles and Responsibilities

All departments and agencies are responsible for safeguarding employees, information, assets and service delivery within their area of responsibility. The guidance on access management provided in this document shall be the minimum baseline for GC departments and agencies.

Tenant organizations are responsible for informing custodian departments and agencies of their security requirements for site selection and tenant fit-up. Custodian departments and agencies are responsible for providing and funding the safeguards considered necessary by the custodian to protect facilities based on a threat and risk assessment (TRA) conducted by or for the custodian. This responsibility includes implementing and integrating measures for base building security (exterior doors and lighting), building systems (elevator, mechanical and electrical systems) and life safety (exit stairs, fire alarms and sprinklers). Custodians are also responsible for integrating tenant-funded requirements in to their building infrastructure.

This guide should be used to support decision making for GC Facilities and are not specific to Remote/Telework locations. Other guides may be required to fully assess Remote/Telework security and are available at Lead Security Agency for Physical Security - Royal Canadian Mounted Police (rcmp-grc.gc.ca).

1.3. Equity, Diversity, and Inclusion in Physical Security Systems

All employees of the Government of Canada (GC) have a responsibility to safeguard persons, information and assets of the GC. It is important that security policies and practices do not serve as barriers to inclusivity, but instead support and respect all GC personnel while ensuring appropriate security measures are maintained for the protection of GC personnel, assets, and information.

Initiatives to promote equality and inclusion among the diverse communities and heritages within the GC, should be respected in the development and maintenance of physical security systems. Departments and agencies should follow all GC legislation, policy and directives on Equity, Diversity, and Inclusion (EDI) in the promotion of a fair and equitable work environment for all persons while ensuring they meet their mandated security responsibilities.

Departments and agencies should conduct a risk management exercise to ensure, that while the dignity of all is respected, the protection of GC information, assets, and personnel is maintained. All questions on EDI policies and directives should first be addressed to your responsible departmental authority.

1.4. Information Technology Considerations

With the constantly evolving threat landscape, and the convergence of physical and information technology (IT) security, the requirement to assess the risk of any application and/or software connected to a network to operate and support equipment in Government of Canada controlled buildings is critical. Some examples of these control systems could be for items such as, but not limited to, security lighting, perimeter gates, doors, HVAC etc.

Before implementing any applications and/or software that will control and/or automate certain building functions, your departmental security requires the completion of a Security Assessment and Authorization (SA&A). This will ensure that the integrity and availability of the components the applications and/or software controls are maintained and that any risks highlighted will be mitigated. Starting the SA&A process early is highly recommended to ensure project delivery schedules are not affected. For more information on the SA&A process, please consult your departmental security.

2. Contact Information

For more information, please contact:

Royal Canadian Mounted Police
Lead Security Agency for Physical Security
73 Leikin Drive, Mailstop #165
Ottawa, ON
K1A 0R2
Email: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronyms

Acronym	Meaning
CCBFC	Canadian Commission of Building and Fire Codes
CCTV/CCVE	Closed Circuit Television / Closed Circuit Video Equipment
CPTED	Crime Prevention Through Environmental Design
CSO	Chief Security Officer
DSM	Directive on Security Management
GCPSG	Government of Canada Physical Security Guide
HSZ	High Security Zone
IT	Information Technology
NFC	National Fire Code of Canada 2020
OZ	Operations Zone
PDRR	Protection, Detection, Response and Recovery
PIN	Personal Identification Number
PGS	Policy on Government Security
PZ	Public Zone
RZ	Reception Zone
SA&A	Security Assessment and Authorization
SOP	Standard Operating Procedures
SZ	Security Zone
TRA	Threat and Risk Assessment

4. Glossary

Term	Definition
Access Card	A device (card) issued by a department or agency to provide authorized individuals access to a particular area or zone within a facility or complex. It should not be confused with an identification card which provides identifying data about a person such as their full name, department or agency, identifying features, of a GC employee.
Asset	Tangible or intangible things of the GC. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.
Authorized Individual	An individual working with the GC, including employees of the federal government as well as casuals, contractors, students and other persons who have been security cleared to access government information, assets, facilities, and/or electronic networks and devices.
Availability	The condition of being usable on demand to support operations, programs and services.
Baseline Security Requirements	Mandatory provisions of the Policy on Government Security and its associated operational standards and technical documentation.

Biometrics	Unique physical characteristics, such as fingerprints, facial, voice, iris, and palm or finger vein patterns that can be used for automated recognition.
Classified Assets	Assets, if compromise could reasonably be expected to cause injury to the national interest.
Classified Information	Information, if compromise could reasonably be expected to cause injury to the national interest.
Compromise	Unauthorized disclosure, destruction, removal, modification, interruption or use of information or assets.
Continuous Monitoring	On a continuous basis, verify security the area or facility remains uncompromised. Examples include electronic intrusion detection systems or someone guarding a particular point on a constant basis.
Control of Access	Ensuring authorized access to assets within a facility or in restricted areas by screening visitors and material at entry points by personnel, guards or automated means and, where required, monitoring their movement within the facility or restricted access areas by escorting them.
Crime Prevention Through Environmental Design	Principle that encourages the use of landscape and/or architectural design to reduce or eliminate criminal behavior.
Custodian	A department or agency that is responsible for administration of federal real property.
Demarcation	Identifying the boundary between zones and providing notice of any zone-specific requirements for entry and exit by use of posted signs.
Departments and Agencies	Any GC department, agency, scientific facility, or associated facility that is responsible for managing federal real property, information, assets, and/or personnel.
Escort or Escorting	An appropriately security cleared GC employee whom is responsible for the continuous supervision of non-security cleared people in areas where a security clearance or status would normally be required to work.
Exit	Means of egress, including doorways, that leads from the floor area it serves to a separate building, an open public thoroughfare, or an exterior open space protected from fire exposure from the building and having access to an open public thoroughfare.
Facility	A facility may be a building (whole or part) and may include its site or land, or may be an area or construct that is not a building. (weapons ranges, agriculture fields).
High Security Zone	area where access is limited to authorized personnel holding the corresponding GC Security Clearance and to pre-approved/screened, properly escorted visitors. Example – area where information and assets classified higher than Secret are processed or stored.
Identification Card (employee)	A document (card) issued by a department or agency that provides identifying data about a person such as their full name, department or agency, photograph, identifying features, as an employee of the GC. It should not be confused with an access card which is a device issued to

	allow employees to access spaces/zones within a GC facility based on their level of access.
Insider Threat	Instances when personnel, authorized to enter or work within a GC facility, engage in deliberate actions against the GC, their employer, or their colleagues. Actions may include criminal activity, physical threats or actions, espionage, subversion, and sabotage.
Integrity	The accuracy and completeness of assets, and the authenticity of transactions.
Mag Lock	Magnetic locking system operating on a continuous supply of electricity. Activated, or unlocked, when power supply is discontinued by designated switch or fire alarm relay.
Monitoring	To watch for or detect action or activities contrary to security policies or standard operating procedures (SOP).
National Interest	Subjects concerning the defence and maintenance of the social, political and economic stability of Canada.
Need-to-Access	A criterion used by the custodian(s) of sensitive information, assets or facilities to establish, prior to providing physical access or entry, that the intended recipient must have access to the space to perform their official duties.
Need-to-Know	A criterion used by the custodian(s) of sensitive information, assets or facilities to establish, prior to disclosure or providing access, that the intended recipient must have access to perform their official duties.
Operations Zone	Area where access is limited to personnel who work within and to properly escorted visitors only. Example – Government office space/staff only warehouse
Periodic Monitoring	Monitoring on a regular basis, but not continuous, to confirm there has not been a breach of security. The frequency and diligence of periodic monitoring is based on a Threat and Risk Assessment.
Protected Information	Information if compromise could reasonably be expected to cause injury to other than the national interest.
Protected Asset	Assets whose compromise would reasonably be expected to cause injury to other than the national interest.
Public Zone	Area where the public has unimpeded access and generally surrounds or forms a portion of a government facility (grounds surrounding a building).
Proximity Card	A device, often combined with an access card, containing a readable chip that communicates with an access control reader, keypad, or biometric reader. Use of this card acts as part of multi-authentication system to allow employees to access spaces/zones within a department or agency based on their level of access.
Reception Zone	Area where the transition from a Public Zone to a restricted-access area is controlled. Example – Reception lobby or Security Guard Post.
Reliability Status	The minimum standard of security screening for positions requiring unsupervised access to GC protected information, assets, facilities or information technology systems. Security screening for reliability status

	appraises an individual's honesty and whether they can be trusted to protect the employer's interests. Security screening for reliability status can include enhanced inquiries, verifications and assessments when duties involve or directly support security and intelligence functions.
Restricted Access Area (RAA)	A work area (site or building) within a department where access is limited to authorized individuals. This includes Operations Zone, Security Zone, and High Security Zones as defined in Ref: GCPSG-015 Guide to the Application of Physical Security Zones
Security Clearance	The standard of security screening for all positions requiring access to GC classified information, assets, facilities or information technology systems. Security screening for a security clearance appraises an individual's loyalty to Canada and their reliability as it relates to that loyalty. Security screening for security clearance can include enhanced inquiries, verifications and assessments when duties involve or directly support security and intelligence functions.
Security Zone	An area to which access is limited to authorized personnel holding the corresponding GC Security Clearance and to properly escorted visitors. Example – area where information classified up to and including Secret is processed or stored.
Tenant	A department or agency occupying federal real property that is under the administration of another department, agency, or Crown Corporation.
Threat Risk Assessment (TRA)	Assessment of a facility to identify risk, threats and vulnerabilities to assets (information, employees, services, etc.).
Unauthorized Access	Access to information or assets by an individual who is not properly security screened and/or does not have a "need-to-know".

5. Access Requirements/Privileges Based on Security Screening Level

A fundamental requirement of the PGS is to limit access to sensitive information and areas. The PGS further restricts access to those who have the need-to-know, or a need-to-access, in order to perform their duties. While security screening levels permit access to certain information or areas, the application of the need-to-know and need-to-access principles restrict that access to those with a requirement to read/know specific information or to access specific areas. Personnel are not entitled to access merely because it is convenient or because it is commensurate with their security clearance level, status, rank, or office. Departments and agencies are responsible to actively review access privileges and should revoke access when it is no longer required (Example: an employee no longer requires access to an area, accepts a position with another department or agency, or when they cease employment in the GC).

An effective way of implementing and maintaining the need-to-know or need-to-access principle consists of segregating and controlling access to sensitive GC information and assets through the effective use of physical security zones. Given that individuals within the GC can pose a threat to the availability, confidentiality or integrity of GC information or assets (often referred to as insider

risk); limiting access only to those with the appropriate need-to-know / need-to-access can reduce the risk of insider threat and help safeguard GC information and assets.

Access management is a process utilizing a combination of physical security hardware and Standard Operating Procedures (SOP) to regulate access to GC facilities, information, and assets. Access should be limited to only those who hold a valid GC Reliability Status or Security Clearance to the appropriate security level, whose duties require them to have such access, and have been approved access by the appropriate authority. These requirements are necessary for authorization to be granted and access management to be effective.

This table identifies the baseline access privileges based on security screening levels. It is important to note that not all departments and agencies are structured the same therefore, some of the screening levels may not be applicable.

Table 1 – Access Privileges

		Visitor (no security Screening)	**Security Screening Levels**		
			Reliability Status (RS)	Secret	Top Secret (TS)
Zone Access	Public	✓	✓	✓	✓
	Reception	✓	✓	✓	✓
	Operations	X	✓	✓	✓
	Security	X[1]	✓[1]	✓	✓
	High Security	X[1]	X[1]	✓[2]	✓ TS with Indoctrination may be required in some HSZs.

LEGEND

✓	Zone access permitted (provided that the individual has the need-to-know or need-to-access).
✓[1]	Zone access shall require an escort with a minimum Secret clearance.
✓[2]	Zone access may require an escort depending on the space. For example, an employee with a Secret clearance can enter a room without an escort (which is a High Security Zone) however, an employee with a Secret clearance cannot enter a Classified Environment room (which is a High Security Zone) without an escort (a Top Secret clearance is needed).
X	Zone access permitted with appropriate escort. Escorted by an authorized employee: • who is a permanent occupant of the space with (at minimum) a valid RS, or • security personnel with a valid RS.
X[1]	Zone access permitted with appropriate escort. Escorted by an authorized employee: • who is a permanent occupant of the space with a valid Secret or Top Secret security clearance, or • security personnel with a valid Secret or Top Secret security clearance.

During periods of increased risk, departments and agencies may be encouraged to implement additional access control measures in order to safeguard their personnel, information, or facilities. Please refer to Appendix A – Responding to Higher Threat Levels for access management options available to departments and agencies.

6. Facility Layout/Zones

Access management is fundamentally linked to the concept of physical security zoning, and control measures between zones, to manage the flow of personnel and goods throughout their organization. Being familiar with GCPSG-015 – Application of Physical Security Zones Guide, will aid departments and agencies in applying appropriate physical security zone(s) in their facilities. The five physical security zones are as follows:

- Public Zone (PZ);
- Reception Zone (RZ);
- Operations Zone (OZ);
- Security Zone (SZ); and
- High-Security Zone (HSZ).

Refer to GCPSG-015 – Application of Physical Security Zones Guide for additional information on physical security zones and additional measures that may be required for specialized security zones and controlled access areas.

Note: **Temporary Zones** - Any establishment of a temporary restricted access zone (OZ, SZ, or HSZ), inside or outside a controlled area, must meet or exceed the same standards used to meet the minimum specifications of a permanent physical security zone for the duration of use of the temporary zone. These temporary zones could be established to house or process sensitive information classified above the level normally stored in the zone, provided:

- the necessary physical security safeguards are in place;
- the increased risk is documented through a formal TRA; and
- the risk is accepted by an organization's departmental security authority (CSO or delegate).

For example, a temporary SZ could be established around a seized vessel or truck under continuous guard; provided personnel, processing sensitive information, positively control access and storage of the asset in accordance with relevant guidance, GCPSG-007 - Transport, Transmittal and Storage of Protected and Classified Material.

Facility design allowing for natural observation, access control, and territorial reinforcement (Zones & Signage) – key components of Crime Prevention Through Environmental Design (CPTED) – enable departments and agencies to manage the flow of individuals throughout a facility. These models intend to positively influence behavior and activities while discouraging undesirable actions by both staff, visitors, and potential adversaries. CPTED has a collection of situational crime prevention principles to be met during the designation, definition, and security design of an environment. The following principles are also discussed in G1-005 Guide to the Preparation of Physical Security Briefs.

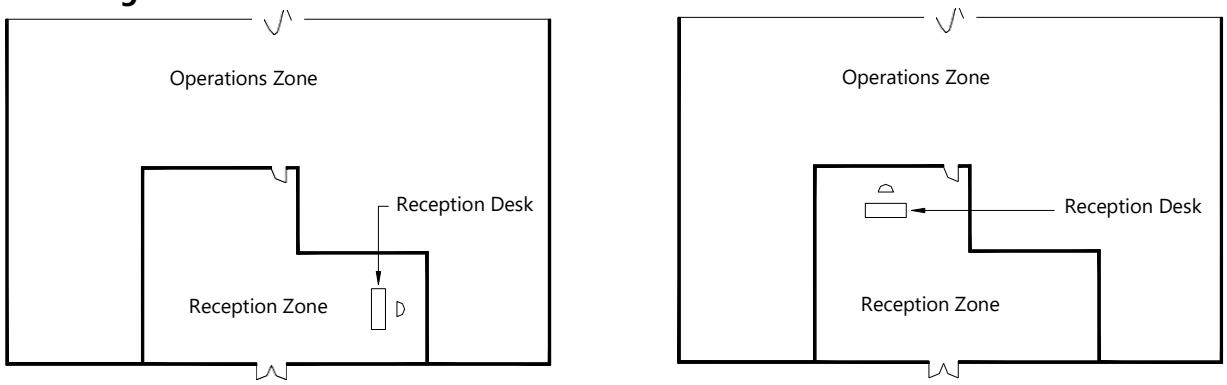
6.1. Natural Observation/Access Control

The CPTED principle of natural observation and natural access control are effective design concepts intended to improve access management of departments and agencies. Natural observation can be achieved by establishing and maintaining clear, unobstructed sight lines that promote easy identification of approaching or transiting individuals and vehicles. Methods of establishing this visual objective may include well-groomed landscaping, clear pathways, security lighting, etc. Natural access control is based on the concept of clearly defined boundaries that influence or control the flow of movement. Some examples of natural access control are perimeter fencing, walking paths from the street to the building door, landscaping (such as shrubs, flower beds, trees, ponds) to act as a barrier (examples include winding roads to slow the speed of vehicles, embedded concrete flower beds to act as anti-ram vehicle barriers).

The primary objectives of natural observation and natural access control are to encourage people to enter and exit the premises in a predictable manner, that is easily monitored, and to discourage unauthorized individuals from attempting to enter out of fear of being easily identified and apprehended.

For example, consider the location of the reception desk in the following two examples:

Figure 1



Example No. 1 Example No. 2

Alt Text Figure 1 depicts a preferred location for a reception desk to allow observation of a lobby

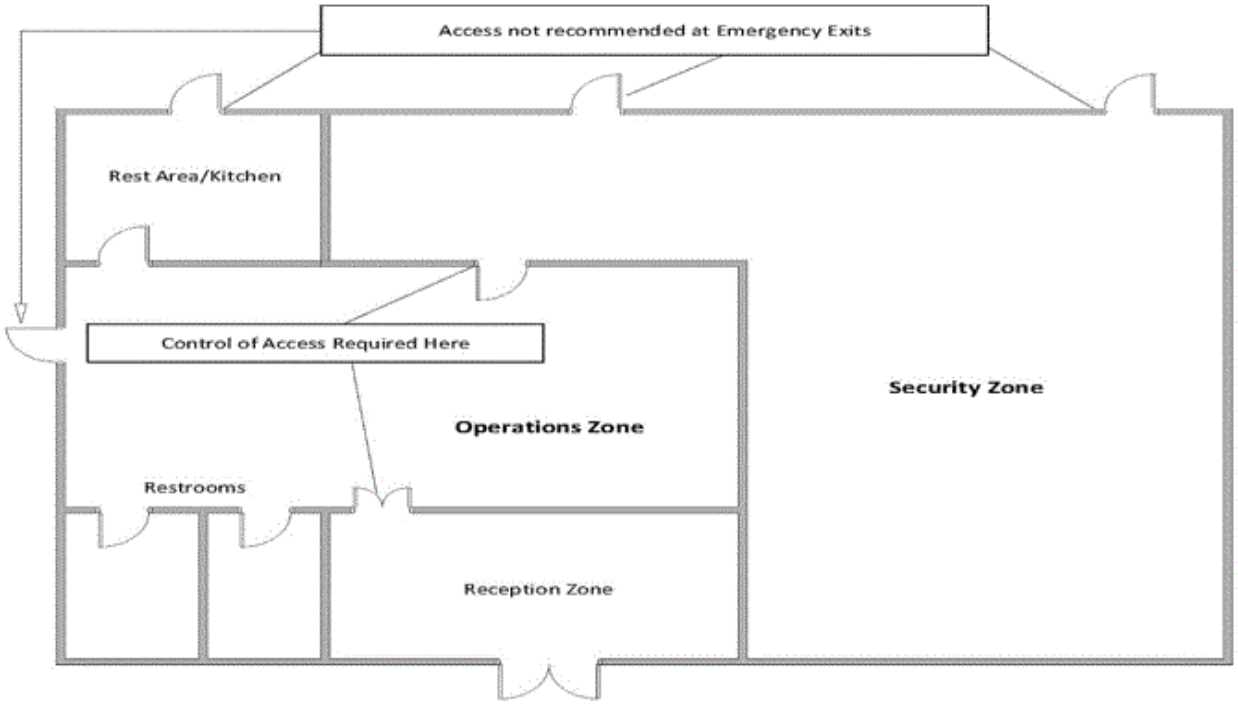
In example number 1, the reception desk cannot see the door between the RZ and the OZ. An individual could wait for an opportune time to enter and might go unnoticed by the employee at the reception desk. In example number 2, the reception desk has been relocated to allow for observation of the entry area. An unauthorized individual would feel more conspicuous if they tried to wait for an opportune time to enter, and would more likely be noticed from the reception counter.

6.2. Compartmentalization (Zones)

Compartmentalization can be defined as the physical separation of an area(s) within a structure in order to promote a sense of ownership or territorial reinforcement, provide opportunities for

natural surveillance of the point of access, and establish a clearly defined sequence of boundaries through which a visitor or departmental employee may or may not pass. Individuals moving between these spaces should perceive the boundaries and understand the rules / limitations associated with crossing into/out of the functional space. For departments and agencies, employment of GCPSG-015 – Application of Physical Security Zones Guide will enable the desired layout.

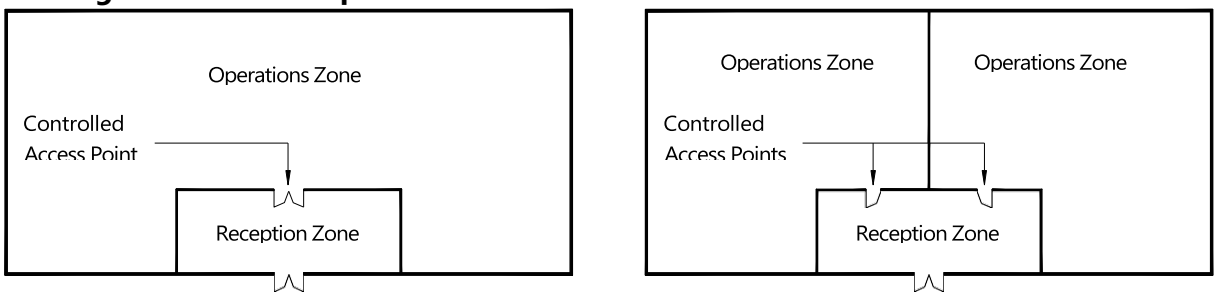
Figure 2 Zones



Alt text Figure 2 depicts a floor plan of a building with different zones where access is controlled to each space.

Compartmentalizing an office can reduce the number of employees who have access to individual assets. In larger departments and agencies, it is usually possible to organize into groups which seldom need to interact with each other to perform their duties. For example, a research and development branch of a department may have no need to interact with a communications branch on a regular basis. Consider the following example:

Figure 3 Internal Separation of Zones



Single Operations Zone Multiple Operations Zones

Alt text Figure 3 depicts the division of Operations Zones to limit access between sections

In Figure 3, the two sections share the entire OZ which could lead to unauthorized access to the information and assets of either section occupying the space. This may lead to additional mitigation measures and costs to safeguard their respective information and assets. Whereas in the Multiple OZ, the OZ has been divided into two self-contained work spaces; thus, reducing the risk of unauthorized access held by either section.

6.3. Demarcation/Signage

Demarcation is identifying the boundary between zones and providing notice (signage) of any zone-specific requirements for entry and exit. Although this can be achieved by way of a line of tape on the floor, a temporary wall such as a room divider, a desk, etc., the best practice is to install physical barriers (doors, walls, etc.) around each separate area to which access is controlled. This in itself may not be enough to discourage individuals from attempting to enter. Without signage, for example, an individual may perceive a locked door as an inconvenience when attempting to enter, rather than as the perimeter of a restricted access zone. The purpose of the signage should be clear in order for it to be respected. See Figure 4.

- At access points, where personnel will enter and exit, identify each area with appropriate signs detailing restrictions and/or entry requirements; such as Authorized Personnel Only;
- Visitors Must Be Escorted;
- No electronic devices; and
- Operations Zone.

Just as importantly, signage to remind personnel they are exiting a higher security zone is a useful tool to remind all to lock security cabinets, not to discuss classified information, or other site-specific security countermeasures employed with departments and agencies.

Figure 4

Alt text Figure 4 depicts an example of signage located at an access point.

Note: Signs should conform to the Federal Identity Program Manual, be fixed in place to enable them to be easily observed on approach, and when possible include pictorial information.

6.4. Fire Safety/Building Code Considerations

Access management systems and procedures must never endanger the safety of personnel within GC properties. Departments and agencies are to make every effort to adhere to applicable legislation regarding building design, composition, fire safety, mobility accessibility, occupational health and safety, etc.

Applicable Canadian legislation should be considered the minimum standard for departments and agencies that are located outside of Canada; however, if local laws are of a higher safety standard or legal threshold, the higher/more prescriptive building safety requirements will be employed. In these instances, physical security and building design/maintenance personnel should work together to develop solutions to satisfy both the employer's responsibility to provide a safe work environment and employees' responsibility to safeguard GC information and assets in accordance with policy.

6.4.1. Emergency Exits

Under the 2020 National Fire Code (NFC), the Canadian Commission of Building and Fire Codes (CCBFC) outlines the minimum physical construction design standards for facility fire safety. Although fire safety systems, such as emergency exits, are necessary for the preservation of life in life-threatening/emergency situations, these exits can also be used to circumvent access control methods described in this guide. Departments and agencies should develop solutions and/or SOP for preventing access via emergency exits based on an updated TRA. As a best practice, emergency exits should be:

- Interior activation (opening) only;
- Well illuminated (GCPSG-004 – Security Lighting Considerations Guide);
- Connected to a monitored intrusion alarm system and/or local audible alarm to alert others the door has been opened; and
- If supported by the TRA, monitored by a CCTV system in co-operation with the intrusion alarm system.

6.4.2. Emergency Power

In order to maintain control of access during a power outage, an access control system must be connected to a backup power source. Ideally, the system should be connected to an emergency power generator which could allow the electronic access control system to function for a longer period of time until wider power is restored. As a best practice, access control systems should be configured to a back-up power supply to allow for uninterrupted access based on a TRA.

Note: Back-up power for access control systems is different than "Mag Locks". Magnetic lock systems should be on a power supply (with batteries) but also employ a fire panel disconnect to shut off power to the mag lock in case of a fire emergency. See 7.5.3 Magnetic Locks.

7. Methods to Control Access

An access control system allows the movement of authorized personnel and material into and out of facilities, while detecting and possibly delaying movement of unauthorized personnel/visitors and items.

The objectives of an access control system used for physical protection are as follows:

- Permit only authorized persons to enter and exit;
- Detect and prevent entry or exit of contraband material (weapons, explosives unauthorized tools or critical assets);
- Provide information to security personnel to facilitate assessment and response (muster report in case of emergency); and
- Incorporate the flexibility to address changes in Threat Levels (Appendix A) and enable a rapid return to normal operations.

In establishing physical security zone design and layouts, the first two zones (PZ and RZ) should establish access conditions for the three restricted area zones (OZ, SZ, HSZ); with the baseline security requirement that access is controlled for the OZ and higher. This is detailed in depth in GCPSG 015 – Guide to the Application of Physical Security Zones.

Since no two facilities are identical, departments and agencies should build upon the following baseline access management principles and develop their own unique countermeasures and SOP that are supported by a TRA. Some commonly used methods of access management can include:

- Identification, access, or combined identification/access cards;
- Physical security hardware (doors and locks);
- Electronic card access systems (proximity cards, coded access control keypads); and/or
- Facility perimeter or boundary access points (vehicle gates, pedestrian turnstiles).

A combination of these may be utilized to increase or strengthen the overall effectiveness of any access management strategy.

7.1. Protection, Detection, Response and Recovery (PDRR)

Departments and agencies should incorporate elements of protection, detection, response, and recovery (PDRR) into their access management strategy. Refer to GCPSG-019 (2023) Protection, Detection, Response, and Recovery Guide, for more information:

- Protection is achieved through the use of physical, procedural and psychological barriers to delay or deter unauthorized access;
- Detection involves the use of appropriate devices, systems and procedures to signal that an attempted or actual unauthorized access has occurred;
- Response entails the implementation of measures to ensure that security incidents are addressed immediately. The response action includes reporting to appropriate security officials and ensures that immediate and long-term corrective action is taken in a timely fashion; and
- Recovery refers to the restoration of full levels of service delivery following an incident.

Departments and agencies' SOP should be clear to ensure that appropriate responses are activated in the event of a detected unauthorized access. These SOP should be reinforced by regular awareness and training opportunities for employees, to ensure the appropriate responses are activated and designated security officials are contacted during security incidents, emergencies, and high-threat situations. Security incidents must be reported to the organization's Security Coordinator by completing and submitting a security incident report. Some examples of access control violations include, but are not limited to:

- Unauthorized access;
- Lost or stolen keys, building access card or ID card;
- Any known or suspected tampering with mechanical security systems and devices; and
- Any known or suspected tampering with electronic security systems and devices.

7.2. Identification and Access Cards

Departments and agencies are required, by the DSM, Appendix C: Mandatory Procedures for Physical Security Control to implement measures to ensure access to GC information, assets, and facilities is restricted to authorized individuals by issuance of identification cards for employees and access cards, for employees and other authorized individuals, to control and monitor access to restricted zones or facilities.

Identification cards are intended to distinguish employees of a department or agency from individuals belonging to another department, agency, or the general public that would require separate authorization and supervision on the premise. Only individuals with a valid GC security clearance and employed by the department or agency shall be eligible for an identification card.

Access cards are intended to grant the bearer entry into any restricted space/zone(s) on a need-to-access principle. Access cards may also be used for contractors, delivery personnel, or visitors to a GC facility.

Departments and agencies may also employ a combined Identification and Access Card for employees; as long as the minimum capabilities, outlined in 7.4 Electronic Access Systems, are met.

Common and unique physical characteristics of identification and access cards are found in Appendix B of this guide. Appropriate uses and best practices are found in Appendix C.

7.3. Mechanical Access Systems

Mechanical measures to control access involve the use of a physical barrier at an entry point. Examples of these barriers include doors, turnstiles and gates. When used for access control, these barriers must be combined with additional means to permit or deny access. This may include reception personnel or security guards, electronic access systems, or mechanical means.

The most common mechanical means for controlling access is the keyed lock. When keyed locks are used for access control, control over who has access to the keys becomes critical. If keys can be easily copied, control of access cannot be guaranteed. Similarly, if a key is lost, lent, or stolen, there is a risk of unauthorized access and the lock must be replaced. If the lost key is a master key, then a greater number of access points will be affected. Nonetheless, if proper key control is maintained by a centralized system, keyed mechanical locks may be an effective and inexpensive method to contribute to managing access.

Combination locks, often in the form of a push button combination pad, are an alternative to keyed locks. These are vulnerable in that unauthorized individuals can learn the combinations; limiting their effectiveness dependent upon the security awareness of users. Combinations must not be written down where they can be found by others. Locks should be positioned to minimize the potential for overview. For additional protection, combinations should be frequently changed.

Further information about locking hardware and key control requirements is described in GCPSG 010 – Operational Physical Security Guide.

7.4. Electronic Access Systems

Electronic access management systems often include a number of features not found in mechanical systems. Some of these features include:

- The capability of identifying and recording where entry was made and with which key or device;
- The ability to permit or deny access depending on the time of day;
- The ability to change permission to access without changing any hardware;
- The ability to monitor the status of a door to indicate whether it is open, closed, locked;
- The ability to indicate unauthorized attempts to access (door open too long, forced entry);
- The capability of linking the key/access card/device to information about the person it is assigned (for example, photograph, employee status, access level granted); and
- The ability to be linked with other electronic security devices such as CCTV. This can also restrict access to different zones only accessible for the specific user.

In some situations, it may be less expensive and more effective to use electronic systems to control access. The most important requirement for electronic systems to be effective is a proper physical design, that is easy to use, is combined with the appropriate compliance by trained users.

Typically, with an electronic access management system the user must present an access card, code, or some other item - referred to as a key – at an entry point, which the system can identify. Components that may be included in these systems are:

7.4.1. Keypads

Typically, a keypad is mounted near an entry point but some facilities may have stand-alone keypads. Authorized users type in their entry code to obtain access. The system is relatively inexpensive but vulnerable if entry codes are generic among all staff, shared by the user, guessed or overseen. Best practices are to employ a Personal Identification Number (PIN) code management system that provides individual PIN codes to each staff member and to use scramble keypads to reduce the likelihood of other memorizing the PIN codes entered on the device.

7.4.2. Electronic Access Cards/Proximity Card Reader

Electronic access cards, or proximity cards, are presented to a card reader at an entry point. A database connected to the reader identifies information about the cardholder, including the right to access that particular entry point. Should a card be lost or stolen, the privileges of that card can be easily changed in the database without modification to the entry point or the reader. Currently, the most common form of electronic access control are access cards used in combination with individual PIN codes or a combined identification/access card.

7.4.3. Biometrics

Biometric devices can ensure that the person requesting entry is not using someone else's access card or code. It does so by requiring the person present a physical characteristic to a reader. This may be an eye scan, a fingerprint, a hand print, or a face which can be recognized and authenticated by the system. Biometric systems are sometimes slow or inconvenient and often more expensive than other systems. They may not work well for all users, since some people have physical characteristics which make it difficult to enroll them in the system. Biometric systems are generally less appropriate for high-traffic areas, and more appropriate when there is a limited number of users and relatively high security requirements to control access. GC departments and agencies should complete a Privacy Impact Assessment (PIA) when considering the introduction of biometric systems.

7.5. Access Control Lock Hardware

In addition to the ability to identify who has the right to enter an area, an electronic access management system will also have some mechanical components of granting that access. These can include:

7.5.1. Electric Locks

Electric locks allow a door handle to retract the latch only when authorized by an access (proximity/chip) card, PIN code, biometric reading, or combination thereof. Normally the door latch is immobile.

7.5.2. Electric Strikes

The strike is the part of door hardware into which the door latch fits. An electric strike system can allow the door, in which the door latch is immobile, to be opened by

releasing the strike without requiring the latch to be retracted. Similar to an electric lock, this activation would require the use of an access (proximity/chip) card, PIN code, biometric reading, or combination thereof.

7.5.3. Magnetic Locks

Some doors are held shut by electronic magnets. The magnet is released when the electric current is removed from the magnet. Although these are very strong, building code and fire regulations restrictions may limit the use and security offered by this type of lock if they interfere with egress during an emergency incident (fire evacuations), as noted in 6.4.2. Emergency Power.

7.5.4. Turnstiles/Airlocks

Similar to full-height mechanical features to physically slow or prevent access, electronically controlled turnstiles and airlocks have the added benefit of remote monitoring (via CCTV or a control room), remote deactivation in the event of an alarm or emergency, and user identification.

The benefit from the use of turnstiles is the reduction of the opportunity to piggyback. Piggybacking occurs when an authorized user enters through a door and, while the door is in the open position, another person passes through without being processed through the system. Access control turnstiles are designed to allow only one person to enter at a time.

Airlocks are comprised of two doors separated by a short hallway or walkway. Typically controlled by an access (proximity/chip) card, PIN code, biometric reading, or combination thereof, only one door can be activated/opened at a time to enter the zone. Airlocks allow for multiple users to enter the space between doors at one time; which allows for higher volume of staff to enter but raises the risk of piggyback incidents. Similarly, if the interior door is opened, for exiting by staff, unauthorized personnel would be able to enter a physical security zone. Departments and agencies should include regular awareness campaigns and training to ensure staff are not defeating their own access management procedures.

7.6. Reception Staff/Guard Services

Use of access management mechanisms and systems provide a 24/7, cost effective means of managing the flow of personnel within a facility; however, the effectiveness of these systems will deteriorate if they are not monitored or managed by staff. Departments and agencies are encouraged to develop SOP delegating roles and responsibilities for personnel assigned to monitor and manage their facility's access management.

7.6.1. Reception Staff

Primarily employed in public interaction role, Reception Staff should be well versed in the facility's access management SOP. This information should include actions to take for:

- Pre-authorized visitors;
- Unannounced visitors/general public enquires;
- Contracted and delivery personnel;
- Law enforcement and emergency services personnel; and
- Staff not holding/presenting their issued identification card and/or access card.

7.6.2. Security Guard Services

If a TRA identifies a security requirement to employ security guards, issues related to guard type (GC employed or contract), duties, training, equipment and safety, should be addressed. As with reception staff, security guards provide flexibility and an extra layer to an access management strategy by acting as the first line defense in a department or agencies' PDRR design.

SOP for access management must be developed, in addition to those listed in 7.6.1, if the following is included in their stated roles and responsibilities:

- Use of metal detection and/or x-ray equipment;
- Use of a mail handling/containment unit;
- Search of persons;
- Search of vehicles;
- Use of and monitoring of CCTV systems; and
- Emergency response (fire, criminal activity, violent incidents, medical emergencies, lockdown, or shelter-in-place situations).

These SOP should also reflect the impacts of higher levels of threat, as noted in Appendix A of this guide.

7.7. Security Escort Principles

Personnel are permitted to enter a GC premise and/or physical security zone if they hold the following:

- A valid GC Reliability Status or Security Clearance with access privilege detailed above in 5. Access Requirement (see Table 1);
- They have a valid need-to-know/need-to-access; and
- They have approval to enter.

Important: Individuals not matching all of these criteria must be escorted by GC personnel that do hold all three (3) criteria.

7.7.1. Escorting Techniques

Security escorts are effective so long as proper techniques are employed by the escorting staff member(s). Best practices include:

- Provide a pre-escort briefing to educate the visitor/contractor/guest on restrictions and other conditions in order to gain access;

- Ensure the escort has the technical, or area-specific, knowledge to recognize unauthorized activities and risk(s) to GC personnel, property, and information (such as server rooms);
- Ensure electronic devices and other prohibited items are surrendered if applicable to the facility or zone;
- Maintain visual contact of the escorted personnel at all times and avoid situations where it may be inappropriate to accompany the individual (for example, toilets). Best practice is to employ same-gender escorts if possible in these circumstances;
- Maintain a register of visitors to the facility. This allows for a proper accounting of those gaining access and can act as a quick reference tool to account for personnel in the event of an emergency (fire evacuations); and
- Maintain a means to communicate with other staff or security personnel, if permitted for the zone.

Important: It is a commonly accepted practice to escort visitors into a physical security zone to meet with GC personnel. Upon hand over of the visitor to the meeting host, that host is now responsible for the continued escorting of the visitor. Departments and agencies must include guidance on these situations in their access management SOP.

7.7.2. Escorting Violations

Any failure to properly escort a visitor/contractor/guest inside a GC facility will increase the risk of compromise to GC information or assets. The following actions and behaviours must not be permitted:

- **No Escort** - Never leave an escorted individual unattended nor permit them to dictate where they will go inside the facility;
- **Distractions** – an escort must remain alert to their surroundings and the individual(s) under escort. Engaging in distractions (reading a book, using a wireless device, conversing with other personnel, etc.) must be avoided;
- **Outnumbered Escorts** – large groups of visitors, or contractors needing to work in different areas, cannot be properly escorted by one person. Best practice is to provide additional escorts to monitor from separate vantage points and/or break the group up into smaller groups that remain together throughout the escort;
- **Discussing GC Information** – any GC information discussed, that is not related to the purpose of the visit, should be avoided. This may constitute an information security breach; and
- **Contractors Escorting Contractors** – unless contracted staff or security personnel hold a valid GC security clearance (Secret/Top Secret), escorting must be limited to the PZ and RZ only. Contracted staff and security guards should have the duties detailed in the service contract and SOP.

8. Security Awareness Programs for Access Management

Departments and agencies should have a security awareness program, in accordance with their TRA, that ensures all employees are aware they are a part of the access management program. SOP and security awareness campaigns, developed by the Security Coordinator should focus on situational awareness which includes, but is not limited to, the following:

- Steps personnel should take when they become aware of persons without authorization in their facilities;
- Prohibit the sharing of identification cards, access cards, and mechanical keys with other individuals;
- Ensure unauthorized individuals do not piggyback/tailgate into any restricted area;
- Be mindful of who is in the vicinity when discussing sensitive information;
- Challenge individuals who are not wearing or displaying an approved access card;
- Ensure doors, that are normally locked, are not propped open or otherwise disabled;
- Ensure alarms are armed when a space is unoccupied, when applicable;
- Ensure doors and security containers are properly secure (locked);
- Report security incidents, including unauthorized access, the theft/loss of identification cards, building access cards, mechanical keys, etc. to their Security Team;
- Inform employees of the appropriate security officers to contact to report security incidents; and
- Perform escort duties as required.

9. References and Related Documents

- Policy on Government Security – https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578.
- Directive on Security Management - https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611
- Directive on Identity Management - https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16577
- Directive on Privacy Impact Assessment - https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308
- Call to Action on Anti-Racism, Equity, and Inclusion in the Federal Public Service - https://www.canada.ca/en/privy-council/corporate/clerk/call-to-action-anti-racism-equity-inclusion-federal-public-service.html
- Directive on the Duty to Accommodate - https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32634
- Guide for Two-Spirit, Transgender, Non-Binary, and Gender-Diverse Employees - https://publicservicepride.ca/guide/
- Federal Identity Program Manual - https://www.canada.ca/en/treasury-board-secretariat/services/government-communications/federal-identity-program/manual.html
- Design Standard for the Federal Identity Program - https://www.canada.ca/en/treasury-board-secretariat/services/government-communications/design-standard/personnel-identification-design-standard-fip.html
- Standard on Security Screening – https://intranet.canada.ca/pol/doc-

eng.aspx?id=28115&section=glossary

- National Fire Code 2020 - https://publications.gc.ca/collections/collection_2022/cnrc-nrc/NR24-27-2020-eng.pdf
- Canada's National Terrorism Threat Levels - https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html
- GCPSG 004 - Security Lighting Considerations Guide (rcmp-grc.gc.ca)
- GCPSG-007 - Transport, Transmittal and Storage of Protected and Classified Material (rcmp-grc.gc.ca)
- GCPSG 009 - Security Fencing Considerations Guide (rcmp-grc.gc.ca)
- GCPSG 010 – Operational Physical Security Guide (rcmp-grc.gc.ca)
- GCPSG 015 – Application of Physical Security Guides (rcmp-grc.gc.ca)
- GCPSG 019 – Protection, Detection, Response, and Recovery Guide (rcmp-grc.gc.ca)

Appendix A - Responding to Higher Threat Levels

In addition to meeting the baseline level of security set out in the Policy on Government Security (PGS), departments and agencies must be able to respond to declarations of heightened security levels. These increased measures are described in the GCPSG-010 - Operational Physical Security Guide and Canada's National Terrorism Threat Levels.

Departments and agencies should consider the following access management safeguards during periods of increased threat and/or when an increase in the threat level is anticipated. These procedures are suggested best practices which should be considered as part of the response to the need for heightened preparedness.

1. Very Low/Low Threat Level

Day-to-day operations are considered the baseline for access management procedures; supported by a TRA. During this period, departments and agencies are encouraged to promote awareness during initial on-boarding sessions, periodic update training or awareness sessions, and practical exercises for employees of all levels of the organization.

Muster reports should also be generated by the department or agency security team and/or the tenant and/or security staff (persons who have access to access control systems) during emergency situations to ensure employee health and safety. This reporting function should be executed during every evacuation exercise to identify gaps in awareness or training and to engrain the accounting of personnel during emergencies into department and agency mindset.

Depending on the emergency, it may be necessary to shelter in place rather than to leave the facility. Examples include extreme weather, violent demonstrations, or an active shooter outside the facility. Every facility should have identified areas/spaces where occupants could gather. These areas are designed with isolated wall structures to provide additional protection from the threat and tend to be inside the structure.

2. Medium Threat Level

During the Medium Threat Level, departments and agencies should consider providing increased vigilance in the application of safeguards used to manage access during the lower levels. Examples of increased vigilance include:

- Provide an increased level of observation at access points where access cards or electronic access controls are used;
- Employ additional guards where needed;
- Ensure that everyone's access card is displayed in full view;
- Change access codes and/or combinations on locks;
- Verify locations of keys and ensure that key control has not been lost; and
- Ensure greater scrutiny in the verification of visitors' identification.

Departments and agencies should also increase vigilance in the screening of incoming packages in order to identify suspicious items. Additional training could be provided to staff on how to identify suspicious packages. The procedures to follow once a suspicious item has been received could also be reviewed to ensure that staff are fully aware of their responsibilities.

3. High and Critical Threat Levels

Departments and agencies should have prepared emergency plans which they could implement during periods of High and Critical Threat Levels. In preparing these plans, departments and agencies should consider the following:

3.1. Personnel Restrictions

Provide access only to essential personnel.

Departments and agencies should consider reducing the number of personnel on site to ensure the safety of as many employees as possible. To accomplish this, departments and agencies could identify individuals who must be on site to maintain essential services, and permit only those people to access the facility. Alternative arrangements could be made for all other personnel, such as reporting to another facility, working from home, or if these alternatives are not available, not reporting to work until notified otherwise.

3.2. Area Restrictions

Restrict access to essential areas only.

In order to provide essential services, access to all areas of a facility may not be required and departments and agencies may wish to restrict outsider access to certain areas. A loading dock, for example, could be considered non-essential during an emergency. Deliveries could be kept away from the facility and delivery personnel told to return at a later date. Access to the loading area would not be permitted except for security personnel.

3.3. Entry Point Restrictions

Reduce the number and increase the level of controls at entry points.

In facilities with a number of perimeter entry points, the control over access can be improved by eliminating some access points. For example, a facility may have electronic access control installed at a front door as well as a side door adjacent to a parking lot. Access through the side door could be removed, and everyone could be required to enter through the front door. The controls at the front door could then be increased to include increased guard presence and verification of all access cards.

3.4. Auditing

Audit access and egress.

A record should be kept of all incoming and outgoing personnel. In addition to providing information about who has had access to the facility and when they were there, the records would indicate who is in the facility during an emergency. This record can produce muster reports in case of emergency.

3.5. Codes / Combinations

Change pin codes / combinations on locks which control access.

Combination locks and pin codes are vulnerable to being learned by unauthorized individuals. This threat is reduced when the combination and/or pin code is changed, and carefully given out only to authorized users. When an increased threat level is declared, this procedure should be repeated to ensure access only by authorized personnel.

3.6. Access Periods

Restrict the time periods for which access is provided.

At Very Low and Low Threat Levels, it may be that providing access to staff outside of normal working hours is an acceptable risk. This should be reviewed at higher Threat Levels, while departments and agencies should consider reducing the number of personnel with access privileges outside of the normal working day.

4. Phase In – Phase Out

Departments and agencies are encouraged to develop plans that incorporate both the increasing and decreasing of measures employed during periods of increased or decreased threat. Any decrease in operational efficiencies from employing countermeasures during a higher threat level, to protect personnel safety, should be limited in duration to prevent complacency and increase adherence among staff. Preparing plans for a gradual reduction in countermeasures, if supported by the environment or TRA, will assist decision makers in achieving this balance.

Appendix B – Identification and Access Card Features

An effective tool to identify individuals authorized to enter a facility, identification and access cards are similar in design and use; but have very separate purposes in access management systems. Departments and agencies must ensure a consistent application of identity management is used in developing their respective identification and access card programs; in support of Treasury Board of Canada Secretariat's Directive on Identity Management, Directive on Security Management (DSM), Appendix C: Mandatory Procedures for Physical Security Control, and Federal Identity Program design standard.

1. Physical Characteristics

As a minimum, identification and access cards for GC employees should contain:

- the individual's name;
- colour photograph or digitized image;
- date of expiry (normally three to five years from date of issue); and
- a number unique to the card.

See Table 2 for information on comparable features.

Additional information fields must ensure each item is justifiable under existing legislation, such as physical descriptors or employee signature. The photograph of the bearer must provide a frontal view of the head/face and upper shoulders.

All information on the cards must be machine-written without erasures or alterations. Departments and agencies may choose to omit a signature on an identification card if based on the TRA or operational needs of the department/agency. On access cards, the facility location can be identified but best practice is to omit location.

Card size for both should be at least industry standard (such as CR80 54mm x 86mm similar to credit or debit cards); while also allowing access cards to be greater in size and an appreciably larger photograph than identification cards if it is necessary to be able to visually check the card from a distance.

Visitor/Escort Required card information can be limited to department/agency name, location privilege(s), date of expiry, and unique card number. These cards are issued and retrieved daily.

2. Security Features

If a TRA indicates additional security features for identification or access cards are required, the security features incorporated must not result in any defects, obscure printed information, nor impede access to machine-readable information. Additional security features include:

- higher ratios of plastic and resin used in the laminate material;
- watermarks and holograms;

- laser etchings/engravings and images visible only under special lighting; and/or
- optical designs which are difficult to alter or manipulate.

Table 2 – Identification/Access Card Features

Information fields	**Identification Card**	**Access Card**	**Combo Card** (ID and Access card)	**Visitor / Contractor / Escort Required**
Individual's name	Must	Should	Must	Can
Individual's signature	Should	Can	Should	Can
Colour photograph / Digitized image	Must	Should	Must	Can
Name of issuing department/ organization	Must	Can	Must	Must
Location privilege - colours, badge shape, codes	Never	Can	Can	Can
Date of expiry	Must	Should	Must	Must
Unique card number	Must	Must	Must	Must
Date of birth	Can	Can (Month and Year only)	Can	N/A

3. Alterations to Access Cards

Departments and agencies may choose to punch an opening in the access card body to enable the card to be worn on a lanyard. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure that card material integrity is not adversely impacted. It is recommended departments and agencies ensure such alterations do not:

- compromise card body durability requirements and characteristics;
- invalidate card manufacturer warranties or other product claims;
- alter or interfere with printed information, including the photo; and
- damage or interfere with machine-readable technology, such as the embedded antenna or chip.

Employees must not make any alterations to their access card or identification card.

Appendix C – Identification/Access Card Management

The following are considered best practices that departments and agencies could employ to increase the effectiveness of their access management programs.

1. Awareness Program

Departments and agencies should have a security awareness program which ensures that all employees are aware of the organization's identification card and/or access card system and their responsibilities in the successful operation of such a system. This program should include:

- familiarization with each type of card (employee, visitor, contractor, etc.);
- access afforded by each type of access card;
- proper use and display requirements;
- responsibilities of the card bearer;
- awareness that identification/access cards and mechanical keys are not shared with other individuals; and
- procedures to follow when a security violation, loss or theft occurs.

2. Card Management

Each department and agency must establish procedures for the proper administration of identification and access cards. These procedures should include the following:

2.1. Handling Procedures

- Establish a process for issuing and recovering of identification and access cards; ensuring a record is kept of the date of issue, the identity of the bearer, the number of the card, expiry/renewal date, and if necessary, the security clearance of the bearer;
- Verify at the time of issuance the individual's identity, approved security clearance level is valid, and complete a briefing on the bearer's responsible use of the identification and/or access card;
- Provide guidelines for withdrawal of identification or access cards for cause (insider threat);
- Ensure retrieval of cards upon termination of employment, contract, or when no longer required. Ensure cards are only serviceable up to the expiry or termination date;
- Ensure all equipment necessary for the activation/issuance of cards are physically protected to a level equal to the classified/protected information and assets that activated/issued cards could be used to access; based on a TRA;
- Ensure that a process is established which will prohibit the removal of access cards from the facility based on a TRA;
- Establish a process to destroy all expired and/or damaged cards and cards; and
- Ensure no single official in the process may authorize and issue an identification or access card to a person.

2.2. Avoid Duplicate Cards

To properly control access into a GC facility, departments and agencies must limit the issuance of identification and access cards to only one of each per person; or a single combination card if using as part of the access management program. Unless supported by a TRA, issuing additional cards increases the risk of unauthorized access due a lack of positive control of these items.

2.3. Photographs

Photographs on access cards should be as large as practical to facilitate a quick visual confirmation of the access card bearer. Head coverings, that are not part of a religious obligation or cultural custom (for example hijab, turban, or Indigenous headdress) should be removed for identification and access card photographs. Eyewear is acceptable to be worn; however, tinted lenses or sunglasses should not be permitted unless the individual has a certified requirement to wear this style of corrective lenses. Photograph backgrounds should be neutral in nature to allow for a contrast from the individual's complexion.

2.4. Expired Cards

To prevent employees from unnecessary denials of access, a renewal program should be built into the card management program. Providing a reminder or scheduling of a renewal six months prior to the identification and/or access card expiry date should prevent this from occurring to staff. Ensure cards are not re-issued until the Reliability Status or Security Clearance is verified and the individual is still entitled to the card(s). After the new card is recorded and provided to the bearer, the expired card should be identified as invalid in the card management system and destroyed.

2.5. Lost Cards

If an identification or access card is found, the finder should return the card to the security desk or applicable point of contact. In the event that an employee loses their identification or access card, they should notify their manager/supervisor and departmental security unit/office immediately. Where possible, the card holder should provide the last time the card(s) was used or was in their possession. The card should be annotated as lost/missing in the card management system, disabled (if it is an electronic access/proximity card), and replaced.

3. Access Card Use

3.1. Display

A policy that requires the cards to be worn around the neck will encourage employees to participate in the control of access procedures. If health and safety concerns are associated with wearing cards around the neck (working around heavy equipment) alternative measures will be required. Lanyards, retractable card reels, snap hooks, or clips used to hold cards should not include identifiable departmental/agency markings.

3.2. Visual Identity/Card Verification

In circumstances when performing visual identity verification of the cardholder may be required, to determine whether the identified individual is eligible to enter, these steps may be applied:

- Determine whether the card appears to be genuine, has not been altered in any way, by analyzing one or more data elements on the card (name, employee affiliation, employment identifier, card serial number, issuer identification, agency name);
- Compare the cardholder's facial features with the photograph on the card to ensure they match;
- Verify the expiration date on the card to ensure it has not expired;
- Compare the cardholder's physical characteristic descriptions to those of the cardholder (optional);
- Collect the cardholder's signature and compare it with the signature on the card (optional); and
- Verify with an authority whether the cardholder should be granted access if necessary (example – name is not on an access list).

3.3. Visitor/Contractor Access Cards

Persons requiring access to the facility/complex should have their identity verified by security staff and deposit a valid piece of government-issued photo identification before being issued access cards. Employees should be required to sign in visitor/contractors, and be responsible for the access card. Unlike an employee access card with a photo, visitor/contractor access cards can be used by a number of individuals. In order to ensure that the cards represent a properly cleared person, effective control over the number and whereabouts of access cards must be maintained.

When the identity of a visitor is in question, it is recommended that the visitor's home organization be contacted to verify their identity. A visitor may request access, claiming that they are from a specific organization (phone company, maintenance or service company). A phone call to that organization, confirming that the person does indeed work for them and has been sent there, would reduce the risk that this person is trying to gain unauthorized entry.

Cards may be issued to visitors/contractors indicating they have been granted a temporary authorization to access an area. They should be escorted in an OZ, SZ, or HSZ unless they have been granted the appropriate security clearance level and have been granted access by the appropriated departmental/agency authority.

10. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-006 (2024) Access Management Guide for approval.

Nattress,Shawn Thomas,000302786 Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2024.01.12 13:48:26 -05'00'

Shawn Nattress, Date
Manager
RCMP Lead Security Agency

Approved

I hereby approve GCPSG-006 (2024) Access Management Guide.

St-Pierre,Andre Vincent,000171484 Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.01.19 13:43:31 -05'00'

Andre St-Pierre, Date
Director, Physical Security
Royal Canadian Mounted Police