Operational Physical Security Guide

GCPSG-010 (2022)

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

Publication Issued: 2022-12-05
Updated:

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Foreword

The GCPSG-010 (2022) Operational Physical Security Guide is an UNCLASSIFIED publication, issued under the authority of Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA). Although UNCLASSIFIED, the access and use of this guide should be limited to Government of Canada (GC) departments and agencies.

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

Reproduction

Effective Date

The effective date of GCPSG-010 (2022) Operational Physical Security Guide is 2022-12-05.

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).

Acknowledgements

This guide, issued with the Approval of Treasury Board Secretariat (TBS) is a replacement for the TBS issued Operational Standard on Physical Security, which was rescinded on 28 July 2019.

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 information on baseline physical security measures. For detailed information, 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 government employees, 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") as directed by policies and regulations, and recommended security control safeguards (indicated by the use of the word "should").

Baseline physical security measures are designed to provide protection against common types of threats that departments and agencies would 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 overseas facilities.

The provisions pertaining to the storage, transmittal and destruction of classified and protected information and assets apply to both government and non-government facilities.

1.2. Applicability, Roles and Responsibilities

All departments and agencies are responsible for safeguarding employees, assets and service delivery within their area of responsibility. The guidance provided in this document is considered the minimum requirements. Departments and agencies are responsible for validating these requirements as they relate to their departmental security needs.

Tenant departments are responsible for informing custodian departments of their security requirements for site selection and tenant fit-up. (See section 7 for further information.)

Custodian departments 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 (ie. exterior doors and lighting), building systems (ie. elevator, mechanical and electrical systems) and life safety (ie. exit stairs, fire alarms and sprinklers). Custodians are also responsible for integrating tenant-funded requirements, both baseline and enhanced, into their base 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. 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 GC 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, Heating Ventilation and Air Conditioning (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
CCTV/CCVE	Closed Circuit Television / Closed Circuit Video Equipment
CSE	Communications Security Establishment
CPTED	Crime Prevention Through Environmental Design
DSM	Directive on Security Management
FFPA	Federal Fire Protection Association
FSA&A	Facility Security Assessment and Authorization
GC	Government of Canada
HSZ	High Secure Zone

LSA	Lead Security Agency (for Physical Security)
OZ	Operations Zone
PDRR	Protection, Detection, Response and Recovery
PGS	Policy on Government Security
PZ	Public Zone
RCMP	Royal Canadian Mounted Police
RZ	Reception Zone
SCIF	Secure Compartmented Information Facility
SDA	Special Discussion Area
SOC	Security Operations Center
SSA	SIGINT Secure Area
SSR	Secure Storage Room
SZ	Secure Zone
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment

4. Glossary

Term	Definition
Asset	Tangible or intangible things of the Government of Canada. 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.
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.
Classified Assets	Assets, whose compromise would reasonably be expected to cause injury to the national interest.
Classified Information	Information, whose compromise would reasonably be expected to cause injury to the national interest.
Compromise	Unauthorized disclosure, destruction, removal, modification, interruption or use of information or assets.
Control of Access	Ensuring authorized access to assets within a facility or 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.
Custodian	The department having administration of federal real property.
Escort or Escorting	An appropriately security cleared person who 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.
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. (ie. weapons ranges, agriculture fields).

Integrity	The accuracy and completeness of assets, and the authenticity of transactions.
Continuous Monitoring	Monitoring on a continuous basis to confirm there has not been a breach of security.
Periodic Monitoring	Monitoring on a periodic but regular basis 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.
National Interest	Concerns the defence and maintenance of the social, political and economic stability of Canada.
Need-to-Know	The principle that there is a need for someone to access and know information in order to perform his or her duties.
Protected Information	Information, whose compromise would 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.
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: G1-026 Guide to the Application of Physical Security Zones.
Tenant	A department occupying federal real property that is under the administration of another department or Crown Corporation.
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. Types of Threat Conditions

The following threats are common to all government departments and agencies. Various events, accidental or intentional, can cause these threats to manifest themselves and produce injury.

5.1. Work Related Violence

Because of their duties or work-related situations to which they are exposed, employees may be subject to oral or written threats, or acts of physical violence (ie. assault as defined in the Criminal Code, intimidation and stalking) by other employees or members of the public. Work related threats could occur at, or outside the workplace while employees are on duty or off duty.

The Canada Labour Code (CLC) recognizes the problem of violence and requires that employees be appropriately protected. The employer (GC) recognizes employees’ right to be free from these types of actions so that they can safely perform their jobs. Violence Prevention Regulations set out the required method of response to internal and external acts of violence and the mandatory roles of the work place parties. Departments and agencies must follow all regulations and legislation when establishing procedures. For further information, departments and agencies should refer to their Labour Relations and Human Resources groups, the CLC and Criminal Code as required.

5.2. Loss of Confidentiality

Unauthorized disclosure of protected or classified material can occur:

- Accidentally through loss or negligence by employees who were granted access to the information;
- Intentionally by individuals who have authorized (i.e. have been properly security screened and have a "need-to-know") access to the information; and
- Intentionally by individuals who gain unauthorized access to information by whatever means, (ie. targeting of protected and classified information by criminal, terrorist or foreign intelligence elements).

The injury to the national interest or to private/non-national interests increases with the sensitivity of the disclosed information. Injury may include damage to the defence, economy, social or political stability of Canada, the compromise of other governments' interests, breach of privacy, liability or financial loss, loss of confidence in the GC, or decrease of government efficiency. Unauthorized disclosure of Secret or Protected C information will create more injury than unauthorized disclosure of Protected A or B information. In addition, some classified or protected information may be more attractive than other information in the same security classification and may therefore require safeguarding above the baseline security controls required for the categorization of information. For further information on security categorization, refer to the DSM - Appendix J.

5.3. Loss of Availability

Theft, fraud, vandalism, cyber-attack and "malicious activity", accidental or intentional loss or damage by employees or members of the public, and natural events (ie. power failure, fire or flood) are likely threats to assets that could deprive the government of their use, and disrupt program and service delivery. Another impact of these activities is the financial or heritage loss to Canadians in terms of replacement costs or the loss of items that are unique. The injury increases with the importance of the assets to Canadians and the federal government.

5.4. Loss of Integrity

Cyber-attack and malicious activity, willful tampering and employee or system error can cause inaccuracy or loss of information, loss of authenticity and alter intended use. This type of attack may damage a national or personal interest. Impacts also include liability, financial loss, loss of confidence in government, and temporary or prolonged inability to govern properly. The injury increases with the categorization of the information or asset.

6. Physical Security Approach

The government's approach to physical security complements other aspects of the PGS. It is based on the theory that the external and internal area of GC facilities can be designed and managed to create conditions that, together with specific physical security control measures, will reduce the risk of violence to employees, protect against unauthorized access, detect attempted or actual unauthorized access and activate effective response and recovery activities.

Physical security strategies are based on the concept of protection, detection, response, and recovery; a design based on a series of clearly discernable zones; control of access to restricted areas; and the capability to increase security during emergencies and increased threat situations.

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

Departments and agencies must ensure that their physical security strategy incorporates identifiable elements of protection, detection, response and recovery (PDRR). Refer to RCMP Guide G1-025 - Protection, Detection and Response, for more information.

6.1.1. Protection

Protection is achieved using physical, procedural and psychological barriers to delay or deter unauthorized access.

6.1.2. Detection

Detection involves the use of appropriate devices, systems and procedures to signal that an attempted or actual unauthorized access has occurred.

6.1.3. Response

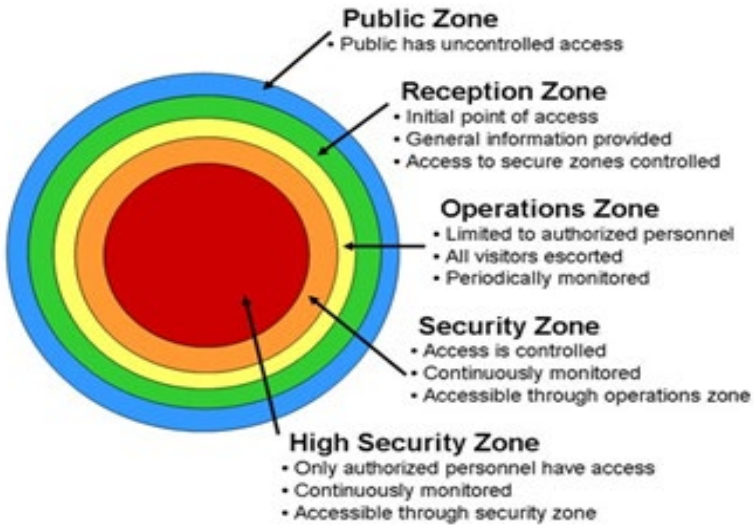
Response entails the implementation of measures to ensure that security incidents are dealt with immediately. The response action includes that these incidents are then reported to appropriate security officials. This ensures that immediate and long-term corrective actions are taken in a timely fashion.

6.1.4. Recovery

Recovery refers to the restoration of full levels of service delivery following an incident.

6.2. Hierarchy of Zones

Departments and agencies must ensure that access to, and safeguards for, protected and classified assets are based on a clearly discernable hierarchy of zones. There are five defined zones: Public, Reception, Operations, Security and High Security Zones:



6.2.1. Public Zone (PZ)

The Public Zone is where the public has unimpeded access and generally surrounds or forms part of a government facility. Examples of a PZ are the grounds surrounding a building, or public corridors and elevator lobbies in multiple occupancy buildings.

6.2.2. Reception Zone (RZ)

The Reception Zone is where the transition from a public zone to a restricted access area is demarcated and controlled. It is typically located at the entry to the facility or space where initial contact between visitors and the department occurs. This can include areas where interaction with security guards occurs, departmental services are provided, or information is exchanged. Access by visitors may be limited to specific times of the day or for specific reasons.

6.2.3. Operations Zone (OZ)

The Operations Zone is an area where access is limited to appropriately security screened personnel who work there and to properly escorted visitors. An OZ must be indicated by a recognizable perimeter and requires periodic monitoring. OZs are a typical open office space, or a typical electrical room.

6.2.4. Security Zone (SZ)

The Security Zone is an area to which access is limited to authorized, appropriately screened personnel and authorized and properly escorted visitors. A SZ must be indicated by a recognizable perimeter and requires continuous monitoring (ie. 24 hours a day and 7 days a week). SZs are areas where Secret information and assets is processed or stored.

6.2.5. High Security Zone (HSZ)

The High Security Zone is an area to which access is limited to authorized, appropriately screened personnel and authorized and properly escorted visitors. It

must be indicated by a perimeter built to the specifications recommended in the TRA, monitored continuously (ie. 24 hours a day and 7 days a week) and be an area to which details of access are recorded and audited. HSZs are areas where high-value assets are handled, or Top Secret information and assets is processed and stored.

The OZs, SZs and HSZs are referred to as restricted-access areas. Instituting a hierarchy of zones allows departments and agencies to:

- Store information or assets of different categorizations or subject to different threats in the same facility;
- Institute varied levels of access control to protect various levels of information and assets;
- Reduce cost by processing and destroying various levels of information and assets within the same facility;
- Select the zones that pertain to the work being done and omit zones when not required; and
- With appropriate planning, changing zones from one period of time to another (ie. changing an OZ during working hours to a SZ during silent hours).

Access to specific zones should be based on the "need-to-know" principle and those holding the appropriate security status or clearance. Restricting access protects information, assets, and employees. Refer to G1-026 - Guide to the Application of Physical Security Zones.

The appropriate number of zones within a facility is dependent on the needs of the department, the number of tenants (single or multi-tenant) and the building owner/custodian (federal, provincial or municipal government or private sector). In a multi-tenant government building, the building or facility security committee (see section 7.7.6) should determine the hierarchy of zones for the common areas. The tenant is responsible for determining appropriate zones within its space.

6.3. Control of Access

Departments and agencies must control access to restricted-access areas using safeguards that will grant access only to authorized personnel. Departments and agencies must also review access privileges periodically and remove access when it is no longer required (ie. when an employee leaves or changes responsibilities, when a contractor completes a project, etc.) Control of access to restricted-access areas and other departmental space must be provided in a manner that does not contravene the life safety requirements of the National Building Code of Canada, National Fire Code of Canada and related codes, standards and guidelines administered by the Federal Fire Protection Association (FFPA).

Balancing effective control of access for unauthorized persons and material while providing convenient access for authorized persons and materials is a challenge for any department. Areas of concern include pedestrian entrances, visitor screening, shipping and receiving areas, parking, utility spaces, mailrooms and corridors leading to restricted zones.

Factors affecting the means of controlling access include such things as the size and location of the facility and the nature of activities undertaken there. For example, the requirement to control access might involve either a series of administrative procedures such as having visitors sign in and out, and having employees show identification badges to security personnel, or a system whereby visitors must contact an employee who would come and escort them into the facility. Facilities with few employees might consider personal recognition techniques to determine authorized and unauthorized individuals entering their space. Departments and agencies should use approved electronic access control technology (ie. card access, PIN access or biometric access control) to meet the requirement for mandatory control of access. A TRA will determine the appropriate cost effective means to control access to a facility.

To facilitate the proper control of access to departmental space, departments and agencies must carefully plan how individuals and material will enter their space. Departments and agencies must have appropriate procedures in place for screening incoming mail/deliveries for suspicious packages. The nature and extent of such screening should be determined by a TRA. For more information, see the RCMP Guide G1-024 - Control of Access.

6.4. Increasing Security in Emergency and Threat Situations

Security safeguards for controlling access of personnel or protocols for managing the risk related to materials must incorporate the need to implement heightened levels of readiness during emergency and heightened-threat situations. Departments and agencies must work with stakeholders to develop scalable security procedures to deal with heightened security or emergency situations such as; armed intruders, protest/demonstrations, or any specific threats to their facilities or personnel.

DSM section C.2.3.4 on additional controls states: Implement additional controls, as required, to meet departmental security requirements or to achieve a higher readiness level in the event of emergencies or increased threat situations. These additional controls include screening of incoming mail or deliveries for suspicious packages, special discussion areas, secure rooms, technical surveillance countermeasures, emergency destruction instructions, and measures for safeguarding sensitive or valuable information or assets.

7. Security in the Selection and Design of Facilities

7.1. Introduction

DSM section C.2.3.1 on the design of the facility environment states: Design, integrate and manage the external and internal environments of a facility to create conditions that together with specific security controls, detect attempted or actual unauthorized entry and activate an effective response to meet departmental security requirements, including electronic surveillance.

Departments and agencies must regularly review their existing facilities as part of their TRA activity to determine whether additional or amended security control measures are needed.

The information provided in this guide is not specific to a particular type of facility nor is it exhaustive. While they are useful for office buildings, they apply equally to other facility types such as GC Co-working facilities, warehouses, laboratories, lands, bridges, wharves and dams. All of these locations require unique security control measures to provide adequate security against the threats identified in this guide and the specific TRA.

The PGS and DSM require departments and agencies to ensure that security is fully integrated early in the process of planning, selecting, designing and modifying their facilities. This may be done through the Facility Security Assessment and Authorization (FSA&A) process (refer to GCPSG-016 - Guide to the Facility Security Assessment and Authorization Process). It is important to ensure that security is thoroughly addressed during all phases of a construction or modification of a project. A multidisciplinary team composed of security officials, occupational health and safety officials, real property experts and program and project managers should determine the appropriate security criteria for each project based on baseline security requirements and a TRA. Departments and agencies must include the necessary security specifications in all plans, request for proposals and tender documents for construction or modification projects and incorporate related costs in funding requirements.

7.2. General Security and Planning

Project managers, real property and security professionals should use information in this section when establishing a security control strategy for a particular project.

7.2.1. Applicable Codes and Policies

Departments and agencies must ensure that physical security measures comply with applicable regulations, codes and policies (ie. Labour, fire, building and electrical regulations and codes and associated Real Property policies).

7.2.2. Emergency Power

Emergency power must be provided for base building services (ie. partial elevator service and emergency lighting). This power must be appropriate for the facilities in order to ensure safe evacuation in the event of an emergency and to protect government assets. A TRA will determine the emergency power requirements for security systems (ie. electronic door locks, CCTV/CCVE, alarms). As a minimum, the emergency power must conform to the National Building Code of Canada and the National Fire Code of Canada.

7.3. Perimeter Security - Considerations for Site Selection

7.3.1. Easements through Site and Emergency Lanes

During site selection and lease negotiation, the possibility of any easements within or adjacent to the facility that could affect the security of personnel or assets must be examined. Easements that permit access to a site by utility crews, the public or emergency personnel limit the tenant's ability to control access; this may result in unauthorized people gaining access to the facility, employees or equipment.

7.3.2. Control of Perimeter

Control of the site perimeter should be achieved through the application of crime prevention through environmental design (CPTED) principles. Examples include keeping intruders under observation through natural surveillance, decreasing crime through natural access control, creating a sense of ownership through territorial reinforcement, and landscape features such as fences, planters and site grading. Other perimeter control measures such as electronic access control, CCTV/CCVE, alarm systems, gates and fences should be considered.

7.3.3. Site Overview, Building Location and Topography

The design, layout and site location of buildings should facilitate natural surveillance by police and the public from the surrounding area (ie. from nearby roadways or other buildings) unless this approach is deemed undesirable by departmental safeguarding strategies. A thorough review of the specific crime statistics for the proposed buildings location must be undertaken to ensure it is appropriate for the buildings intended function. Departments and agencies must also refer to FFPA with respect to the suitability of the facility in the event of an emergency evacuation.

7.3.4. Emergency Services

Firefighting water capacity and the effective response times of firefighters and police must be considered during the development of safeguarding strategies. These must be based on protection, detection and response principles that apply to site selection, facilities and assets. Alternative or additional measures for life safety and asset protection may be required to compensate for inadequate emergency response times. Departments and agencies must seek and follow the direction of the FFPA with respect to the water supply requirements for firefighting.

7.3.5. Adjacent Occupants and Use

Consideration should be given to adjacencies (occupants, tenants and building use) during site selection. This should include the potential impact of adjacent occupants on the safety of departmental employees and on service delivery. Consideration should also be given to the impact of departmental operations on adjacent occupants whether governmental or non-governmental.

7.3.6. Illumination of Site

Lighting should provide sufficient illumination in and around facilities to allow the detection and observation of people approaching the facility, discourage opportunistic criminal activity, address any other security threats that may apply (ie. vandalism and work-related violence) and support surveillance features (ie. natural surveillance and CCTV/CCVE). The choice of light levels must be based on applicable regulations, camera technology and other security considerations. Refer to RCMP Guide GCPSG-004 - Security Lighting Considerations Guide for more information.

7.3.7. Exterior Signage

Signs that identify facilities occupied by federal government departments and agencies must comply with the Federal Identity Program. In addition, facilities should display signs that give clear directions for the site's emergency muster points, parking, visitors, employees and service areas. Consider any conditions or regulations imposed by provincial, territorial or municipal law (ie, regarding CCTV/CCVE or to prove trespass) when using signs to define the boundaries of government property or establish restricted-access areas in accordance with a TRA.

7.3.8. Landscape Design

Landscaping should use CPTED principles and support protection of the building, detection of intruders, and response to security incidents. Landscape security features may include:

- Clearly marked boundaries;
- Fences, walls and other barriers;
- Circulation routes designed to promote natural surveillance;
- Limited natural cover opportunities available for intruders;
- Unobstructed views for security personnel, employees and public of potential problem areas (ie. where criminal activities might occur); and
- Avoidance of materials and furniture that expose the facility to increased risk during a heightened state of security (ie. if a demonstration turns violent).

CPTED principles also include decreasing crime opportunities through natural surveillance, natural access control, creating a sense of ownership through territorial reinforcement and the use of landscape features like fences, planters and grading.

7.3.9. Parking

A TRA or assessment determines the safeguards to protect employees in on-site GC parking areas. These may include placing designated parking areas close to the facility, the addition of security lighting, security fencing, formal escorts, or the institution of a buddy system where employees are accompanied to their vehicles.

7.4. Entry Security

7.4.1. Pedestrian Entrances and Entrance Lobbies

One way of physically controlling access to a facility or its restricted access areas is through the use of entry points. An entry point channels traffic at the facility (including employees and visitors) in a way that permits effective monitoring, screening or control by personnel, guards or automated means.

7.4.2. Service and Utility Entry and Exit Points

Service and utility entrance and exit points (such as air intakes, mechanical ducts, roof hatches and water supplies) must be safeguarded to ensure that the facility's critical assets, life safety measures and departmental programs are not compromised by unauthorized or uncontrolled access.

7.4.3. Shipping and Receiving Areas, Loading Docks and Mail Rooms

Where possible, shipping and receiving areas, loading docks and mail rooms should not be directly linked or adjacent to restricted-access areas or critical facility infrastructure (ie. water mains, cooling and heating systems, fire detection and alarm systems, electrical, telephone and data lines, and other service connections).

7.5. Interior Security - Planning

7.5.1. Circulation Routes, Internal Corridors and Elevator Lobbies

Circulation routes that allow employees and visitors access to restricted-access areas must be carefully planned. This ensures life safety requirements are met, and that access control to restricted-access areas can be maintained.

Planning the location of and activities related to, protected and classified information and assets must ensure that the required safeguards are not compromised during emergencies. For example, a HSZ located on a crossover floor in a high-rise building could require that unauthorized persons pass through it to gain access to a second stairwell during an emergency. Other areas, which require a balance between life safety and physical security, include elevator lobbies, corridors, and limitations on the use of specific locking hardware. RCMP Guide G1-024 Control of Access, Appendix A provides Best Practices related to zoning and building layout, compartmentalization, crossover floors, access to exits, etc.

Access by employees and visitors to restricted-access areas should be based on the individuals' duties and functions, security clearance or status, and the principle of "need-to-know" taking into consideration possible overviewing and overhearing.

The circulation routes followed by employees to transport valuable assets should be planned in a way that addresses the threats identified in the TRA including those identified in Section 5.

Where applicable, access to tenant space from elevator lobbies must be controlled in respect of employees, contractors, visitors and service personnel. Safeguards vary, depending on the nature of departmental programs, the size of tenant space and the number of people requiring access to a floor. They might include a physical barrier such as a wall, an arrangement using personnel, such as a security guard or a reception function, an electronic or mechanical access control system such as a keypad or keys, and security procedures such as limiting elevator use to authorized personnel or having employees challenge people.

7.5.2. Daycare Centers

When daycare centers are located in GC facilities, consideration must be given to the safety of both the tenants and the public in the context of the GCs responsibilities

and liability. Daycare centers should not be co-located with departments and agencies whose programs or operations may be subject to interruption or increased threats due to events such as protests or demonstrations, or within departments and agencies that might deal with high-risk clients (including potentially violent individuals). GC departments and agencies with daycare centers in the facility should have specific sections within their emergency plans to ensure the protection of the daycare center.

7.5.3. Stairwells and Elevators

Stairwells and elevators should not provide direct access to the tenant's restricted-access areas or to critical facility infrastructure. Where possible, passenger and freight elevators (including those from parking and loading dock areas) should open into a PZ or RZ, such as the ground floor elevator lobby. However, elevators or stairwell exits may open into tenant space, if such access is monitored continuously by the tenant, or if the space is secure at all times.

7.5.4. Washrooms

Employee safety must be considered when determining the location of employee and public washrooms. When recommended by a TRA, employee washrooms should not be accessible from PZs or RZs and public washrooms should never be accessible from OZs or SZs.

7.5.5. Amenity Spaces

Consideration must be given to employee safety during the design and layout of common amenity spaces (ie. gymnasiums, food service areas, meeting rooms or conference facilities). It should not be necessary for personnel to enter or pass through any restricted-access zones in order to access a common amenity space.

7.5.6. Telecommunications Wiring Within a Facility

A TRA should be used to determine appropriate physical security measures for telecommunications wiring within a facility. Additional information can be found in the Policy on Service and Digital.

7.6. Controlling Restricted Access Areas

Departments and agencies have several choices available to control access to restricted-access areas. These are personal recognition, access ID badges, mechanical measures (ie. keys), electronic control of access, etc. The appropriate choice will depend on the location of the building, number of employees, TRA etc. Refer to RCMP Guide G1-024 Control of Access for more information on methods to control access.

7.6.1. Identification (ID) Cards / Access Badges

All government employees must be issued an identification (ID) card, which as a minimum includes the bearer's name and photo, a unique card number and an expiry date. Access badges indicate authorized employees and visitors. Where personal

recognition or escorts are not feasible, a temporary access badge must be issued to all visitors (including non-authorized employees, contractors, service personnel) which clearly identifies them as a non-employee. ID cards and access badges may be combined into one single card. Refer to RCMP Guide G1-006 - Identification Cards/Access Badges, for more information.

7.6.2. Electronic Access Control

An electronic access control is a safeguard that assists in controlling access to a facility. A TRA will assist in determining the need and cost effectiveness of such a system.

7.6.3. Closed Circuit Television/Video Equipment (CCTV/CCVE)

CCTV/CCVE equipment may assist a department in monitoring access to their facility. A TRA will assist in determining the need for CCTV/CCVE system. Any specifics of video retention, storage, use or release should be a part of the TRA process and may require research into local laws and regulations.

7.6.4. Security Operations Centre (SOC)

A SOC, whether proprietary or off site, is a focal point for monitoring the various systems such as an electronic access control system, an electronic intrusion detection system and CCTV/CCVE. The SOC will typically include other personal or life safety equipment such as the fire alarm panel. Large departments or complex facilities may require a full SOC however, a smaller version of a SOC may be necessary in all GC facilities. Refer to GCPSG-003 Security Operations Centre Design Considerations Guide.

7.6.5. Special Discussion Areas (SDA)

An SDA is an area designed and managed to prevent the overhearing of Protected and Classified information at various levels of sound attenuation. Owing to the cost of building and operating an SDA, departments and agencies should carefully assess the need, the risk, and cost-effectiveness of options. When construction and use of an SDA is considered, consult the GCPSG-017 - Special Discussion Area Construction Guide or the RCMP LSA.

7.6.6. Secure Storage Rooms (SSR)

Secure storage rooms (SSR) are rooms constructed according to specific technical standards. An SSR may be used for open shelf storage of Protected and Classified material, which would normally require an approved security container. Using an SSR for storage removes the need to use an approved security container only if the "need-to-know" principle is not a concern. Refer to RCMP Guide G13-001 – Secure Storage Room Guide for construction specifications. Where departmental function or a TRA requires, an SSR may be appropriate for the storage of material of evidentiary value during investigations or when awaiting presentation in court.

7.6.7. Security Guards

If a TRA identifies a security requirement to employ security guards, issues related to guard type (proprietary or contract), duties, training, equipment and safety, should be addressed.

7.7. Facility Management

7.7.1. Leasing and Other Occupancy Agreements

DSM section C.2.7 Arrangements states: Establish documented arrangements (for example, lease or occupancy agreements) that define pertinent security requirements and respective security responsibilities where the department relies on or supports another organization, including but not limited to other federal departments, other orders of government, and private sector suppliers and partners, to meet departmental physical security requirements

Physical security requirements for facilities must be included in any leases and other occupancy agreements.

For other information, refer to DSM:

- C.2.7.1 for facilities where the department is the building custodian;
- C.2.7.2 for facilities where the department is a tenant;
- C.2.7.3 for multi-tenant facilities occupied or managed by the department; and
- C.2.7.4 when individuals from another department or organization require regular access to facilities occupied or managed by the department

7.7.2. Cleaning and Maintenance Services

Where cleaning or maintenance is required during limited access hours the custodian should be the contract authority.

7.7.3. Interior Signs

There should be at least one prominent sign inside the main entrance to facilities that directs visitors to the Reception Zones of federal tenants. Signs that identify facilities occupied by federal government departments and agencies must comply with the Federal Identity Program.

7.7.4. Locking Hardware and Key Control

Commercial grade hardware should be used for all locks. In addition, a complete keying protocol should be implemented for the facility, which includes key control and key accountability. Locks on perimeter doors should be keyed separately from other locks, and they should not enable access with a master key. It may also be desirable, especially in larger facilities to limit the use of master keys on janitorial closets and other similar spaces

Keys for the entire facility, spare keys and the information needed to reproduce keys

should not all be stored in the same container. Master keys should not leave the building and not be marked to identify the building for which they provide access. Main and secondary building entrances, SZs and HSZs must not be part of the master keying system.

7.7.5. Renovation Work

When renovation work is needed within restricted-access zones, there should be advance consultation between security and real property officials of custodian and tenant departments. Consultations should include details on security arrangements for access by contractors, which are acceptable to the tenant in order to ensure the safety of staff and prevent the compromise of information or assets.

7.7.6. Building or Facility Security Committee

In multi-tenant facilities, a security committee chaired by a major tenant or the custodian should be organized to coordinate all custodian and tenant requirements for control of access and to plan additional safeguards for heightened security situations. The tenant representatives should be authorized by their departmental security officers to make planning decisions for security measures such as guard services.

8. Storage

8.1. General

Protected and classified information should be stored in approved containers and in the appropriate restricted-access areas. Protected and classified assets, (ie. classified research and development equipment, engineering models or prototypes) should be stored in containers approved for that purpose. For specific guidance on storage, refer to RCMP Guide GCPSG-007 – Transport, Transmittal and Storage of Protected and Classified Material. For requirements not met by GCPSG-007, this guide or by items listed in the G1-001 - Security Equipment Guide, contact the RCMP LSA.

Consider appropriate safeguards to ensure that classified and protected information and valuable assets (ie. laptops) are protected when occupants are away from their workplaces for any length of time.

8.2. Security Containers

When different levels of protected or classified material is stored together, storage must comply with the standard set for the most sensitive asset involved. The infrequent storage of a relatively small amount of assets having a higher categorization level with a larger amount of assets with a lower categorization level may not warrant enhanced safeguards. Classified information should not be stored with valuable assets such as monetary instruments (cash) or drugs in the same security container. Briefcases are not storage containers, and should not be used as such. Refer to RCMP Guide G1-001 - Security Equipment Guide.

Departments and agencies should develop procedures for the storage of assets shared with them from other GC departments and levels of governments, foreign governments, international, educational and private sector organizations. These procedures must be in accordance with international agreements or arrangements between the involved parties and the PGS.

All employees working off-site must safeguard information as per the minimum requirements outlined in RCMP GCSPSG-008 - Physical Security Considerations for Remote and Telework Environments. Employees should also consult the TBS Policy on Telework. With respect to off-site contract work, departments and agencies should use the Security Requirements Checklist (TBS/SCT 350-103) to define the contract requirements and consult with Public Service and Procurement Canada (PSPC) Contract Security Program for appropriate safeguarding or protected or classified assets at contractor facilities.

Access to the contents of security containers must be restricted to:

- Individuals who possess a security status or clearance commensurate with the categorization of material stored within the container; and
- Have a "need-to-know" / "need-to-access" the material stored within the container.

8.3. Valuable Assets

Valuable assets must be afforded protection against loss, destruction or alteration. The degree of protection afforded is dependent on the value of the asset itself and the TRA. Some protection measures are contained in the RCMP Guide G1-001 - Security Equipment Guide. Additional information can be obtained by contacting the RCMP LSA.

8.4. Keys for Security Containers

It is important to understand that "keys" in the context of this section includes mechanical keys, combinations, access cards, and personal identification numbers (PIN). Keys for security containers should be safeguarded commensurate with the highest categorization of the information or asset to which the key provides access. This requirement also applies to records that would allow the reproduction of a key.

Keys that provide access to security containers should be changed for any of the following reasons:

- Annually;
- Anytime there is evidence of compromise;
- If a TRA indicates a change in the level of risk; or
- An employees' need to access the security container has changed.

A record of all changes to keys for security containers should be kept, including: the date, reason, custodian, location and, if applicable, lock identifier, combination number, duplicates, etc. This record of change should be secured commensurate with the highest security level of the information/asset being protected within the container.

8.5. Disposal or Recycling of Security Containers

Departments and agencies are responsible for the disposal of security containers. Approved high security containers for Protected C and classified information must not be disposed of or resold to private sector or outside agencies. Refer to RCMP G1-001 – Security Equipment Guide for more information.

The department is responsible for ensuring that prior to disposal or recycling, all containers are stored in an operations zone as a minimum, all contents have been removed and record logs have been amended accordingly.

8.6. Service and Maintenance of Security Containers

Departments and agencies must ensure that approved storage containers are properly maintained at all times. Refer to RCMP Guide G1-001 - Security Equipment Guide.

9. Transport and Transmittal

Maintaining authorized access to protected and classified material is paramount when it is being transported. When transporting protected and classified assets from one person or place to another, safeguards must include controlling access to the information by "need-to-know". This also applies to the servicing of containers. Departments and agencies are responsible for safeguarding security equipment (ie. security containers) during transport for servicing requirements.

When transmitting protected and classified assets from one person or place to another, protection depends on proper packaging, an appropriate and reliable postal or courier service (government or private sector) and the anonymity of the information while in transit. For protected and classified assets that are at higher risk, appropriate additional safeguards should be used, as indicated in the TRA.

Departments and agencies must transport or transmit protected and classified assets according to the minimum requirements. Detailed specifications for enveloping, addressing and courier services for transporting and transmitting protected and classified assets are set out in RCMP Guide GCPSG-007 – Transport, Transmittal and Storage of Protected and Classified Material.

10. Destruction

10.1. Storage of Protected and Classified Waste

Protected and classified assets awaiting destruction, on or off-site, must be stored at minimum in approved security containers or appropriate secure room. Departments and agencies must safeguard information in transit to a destruction facility in the manner prescribed for the highest level of classified or protected information involved. Refer to RCMP Guide GCPSG-007 – Transport, Transmittal and Storage of Protected and Classified Material.

10.2. Destruction of Assets

Departments and agencies must establish procedures that will ensure security for the protection of protected and classified assets and valuables awaiting destruction. These procedures include:

- Informing staff of the highest levels of protected and classified information that can be destroyed by the equipment within the office;
- Ensuring that authorized personnel are present to monitor the destruction of protected and classified assets and valuables; and
- Segregating protected and classified information awaiting destruction away from non-sensitive information.

10.3. Destruction of Information

Departments and agencies must establish procedures that will ensure security for the protection of protected and classified information awaiting destruction. These procedures include:

- Protected and classified information with no historical or archival value for which the retention period has expired, must be destroyed without delay including surplus copies, draft copies and waste;
- Departments and agencies must ensure that anyone who performs or witnesses shredding is security screened commensurate with the highest level of information being destroyed;
- Departments and agencies should ensure they receive a certificate of destruction for all material destroyed by a third party; and
- Departments and agencies are responsible for ensuring that the shredded material conforms to the size standards noted in RCMP Guide GCPSG-001 – Equipment Selection guide for Paper Shredders.

10.4. Destruction of Electronic Storage Media

For guidance on the disposal and destruction of electronic storage media, refer to Communications Security Establishment Canada (CSE) Information Technology Security Guidance ITSAP.40.006 – IT Media Sanitization.

10.5. Emergency Destruction

Domestically or abroad, where the likelihood of emergency destruction is high or where policy requires it such as a SIGINT secure area (SSA) or Secure Compartmented Information Facility (SCIF), there must be local orders for the prompt destruction of Top Secret and Secret information when its secure transport or transmittal to Canada or an alternate location is not feasible. These orders should be reviewed periodically and kept in a location known to authorize personnel for access during an emergency. Orders should specify that:

- All destruction equipment is properly maintained;
- Sufficient numbers of authorized personnel know how to use the equipment; and
- Priority lists for destruction are updated regularly and are available.

11. References and Related Documents

Directive on Security Management- Canada.ca

G1-025 Protection, Detection and Response - Royal Canadian Mounted Police (rcmp-grc.gc.ca)

G1-026 Guide to the Application of Physical Security Zones - Royal Canadian Mounted Police (rcmp-grc.gc.ca)

G1-024 Control of Access - Royal Canadian Mounted Police (rcmp-grc.gc.ca)

G1-006 Identification Cards / Access Badges - Royal Canadian Mounted Police (rcmp-grc.gc.ca)

Security Operations Centre Design Considerations Guide (rcmp-grc.gc.ca)

GCPSG-017 Special Discussion Area Construction Guide

G13-01 Secure Storage Rooms (SSR) - Royal Canadian Mounted Police (rcmp-grc.gc.ca)

GCPSG-007 – Transport, Transmittal and Storage of Protected and Classified Material

Equipment Selection Guide for Paper Shredders (rcmp-grc.gc.ca)

GCSPSG-008 - Physical Security Considerations for Remote and Telework Environments

ITSAP.40.006 – IT Media Sanitization

Policy on Service and Digital

Canada Labour Code (R.S.C., 1985, c. L-2)

Work Place Harassment and Violence Prevention Regulations (SOR/2020-130)

12. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-010 (2022) Operational Physical Security Guide for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2022.12.05 10:49:09 -05'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve GCPSG-010 (2022) Operational Physical Security Guide.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2022.12.08 11:28:26 -05'00'

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

Date