Protection, Detection, Response, and Recovery Guide

GCPSG-019 (2023)

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

Publication Issued: 2023-12-15
Updated: YYYY-MM-DD

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Foreword

The Protection, Detection, Response, and Recovery 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-019 – Protection, Detection, Response, and Recovery Guide is 2023-12-15.

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 departments and agencies with information on the Protection, Detection, Response, and Recovery model to assist in the development of physical security systems, programs, and standard operating procedures. These measures support operational security, the safety of personnel, and business continuity efforts to facilitate the continued delivery of services throughout a security incident.

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 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" 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.

Some departments and agencies or operational activities may face different threats due to 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

This guide applies to all GC facilities, as departments and agencies are responsible for safeguarding employees, assets and service delivery within their area of responsibility. The guidance provided in this document is intended for Chief Security Officers (CSO), directors, managers, and security personnel who are responsible for the design, operation, and protection of GC facilities and personnel.

Tenant departments are responsible for informing custodian departments of their security requirements for site selection and tenant fit-up.

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 (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, both baseline and enhanced, into their base building infrastructure.

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 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/Abbreviation	Meaning
ACP	Alternate Command Post
ASDP	Alternate Service Delivery Point
CCTV	Closed Circuit Television (Including Closed Circuit Video Network)
CPTED	Crime Prevention Through Environmental Design
DSM	Directive on Security Management
GCPSG	Government of Canada Physical Security Guide
HSZ	High Security Zone
IT	Information Technology
OZ	Operations Zone
PDRR	Protection, Detection, Response and Recovery

PGS	Policy on Government Security
SA&A	Security Assessment and Authorization
SOC	Security Operations Centre
SOP	Standard Operating Procedures
SZ	Security Zone
TRA	Threat and Risk Assessment

4. Glossary

Term	Definition
Adversary	An individual or group intentionally harming, directly or indirectly, GC personnel, departments or agencies. Most often this is in the form of trespassing or criminal activity but can also be actions up to and including terror or state-sponsored violence.
Alternate Command Post (ACP)	A separate location to house and operate an Emergency Response Team or management personnel in the event the normal work space is unavailable due to an emergency event or crisis.
Alternate Service Delivery Point (ASDP)	A separate location to house staff to continue providing services to clients or the general public. ASDP should not be co-located with a department or agency's ACP in order to avoid interference with the management or command structure during an emergency or crisis situation.
Armed Intruder	Life threatening emergency of one or more individuals attacking others with the intent to cause grievous bodily harm or death. Originally defined for attackers use of firearms but also includes bladed weapons (knives, swords), chemical weapons (acid), and other weapons (clubs, vehicles).
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.
Authorized Individual	An individual working with the Government of Canada, 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.
Classified Assets	Assets, whose compromise would reasonably be expected to cause injury to the national interest.
Compound	A site or campus with multiple structures secured as a single entity.
Compromise	Unauthorized disclosure, destruction, removal, modification, interruption or use of information or assets.

Continuous Monitoring	To confirm on a continuous basis that there has not been a breach of security. 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 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.
Defense-in-Depth	This is the principle where security zones are implemented in a progressively restrictive manner, proceeding from the least restrictive zone to the most restrictive.
Delay	The time to defeat a security layer after initiation of the attempt.
Deter	The ability to prevent an attack on a security layer due to perceived difficulty and/or threat of a response.
Departments and Agencies	Any department, agency, scientific facility, or associated facility that is responsible for managing federal real property, information, assets, and/or personnel.
Electronic Intrusion Detection	A system consisting of sensors that detect a change in state (motion, electric current, heat, passcodes), conveys messages to an electronic monitoring program or notification equipment (alarm bell, switchboard, remote access software), and permits analysis of the reported change in state (audible alarm, Security Operations Centre, call-tree/electronic notification).
Emergency Response Team	Management structure within a Business Continuity event or crisis. Also referred to as an Incident Command Structure.
Escort or Escorting	An appropriately security cleared employee 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.
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	Something that is built, installed, or established to serve a particular purpose. A facility may include a specific building (whole or part) or the site or land it is located on. The term encompasses both the physical object and its use (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.
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.
Insider Risk	A person with knowledge of, or access to, an organization's infrastructure (both physical or computer networks) who maliciously, or by misuse of their trusted access, harms the organization's employees, customers, assets, reputation or interests.
Intruder	Any unauthorized individual(s) that have entered into a controlled space contrary to access management procedures.
Lockdown(s)	A set of actions to prevent personnel from entering or exiting a space due to a personal safety emergency. Most often caused by threats of physical harm to personnel inside.
Monitoring	To watch for or detect a breach of security
Need-to-Access	The principle that there is a need for the person to access the area or zone in order to perform their duties. This is not to be confused with the need-to-know the content of the information contained or processed within that area or zone.
Need-to-Know	A criterion used by 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 his or her 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
Penetration Test	An exercise to test the effectiveness of security systems by attempting to physically circumvent the established Access Management and Protection, Detection, Response, and Recovery systems employed in a facility.
Perimeter	A continuous security line surrounding a secured zone.
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.
Physical Security	The use of physical controls to prevent and delay unauthorized access to assets, detect attempted and unauthorized access and activate appropriate response.
Protected compound	A compound where the building(s) and/or assets require additional security controls for the protection of the people, information, or assets contained therein.

Resilience	An ability to withstand or manage a sudden increase in risk or hazard to a person, procedure, or real property. Example: a back-up power supply capable of providing electricity for an extended period of time in the event of a power grid loss.
Risk	The effect of uncertainty on objectives. It is the expression of the likelihood and impact of an event with the potential to affect the achievement of an organization's objectives
Safeguards	Assets or external controls that reduce overall risk to employees, other assets or service delivery by decreasing the likelihood of a threat event, reducing the probability of compromise, or mitigating the severity of the outcome through direct or indirect interaction with asset values, threats or vulnerabilities.
Security Assessment and Authorization (SA&A)	The SA&A is to verify that the IT security requirements established for a particular system or service are met and that the controls and safeguards work as intended. The authorization component is to signify that management has accepted the residual risk of operating the system or service and authorized the system or service to operate based on the evidence.
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.
Standard Operating Procedure	A written set of instructions outlining step-by-step actions to take in order to complete a task(s) and/or respond to an incident. SOP are intended to standardize performance and compensate for any lack of knowledge or experience.
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".
Vulnerability	An inadequacy related to security that could increase susceptibility to compromise or injury.

5. Protection, Detection, Response, and Recovery

The Government of Canada's approach to physical security compliments other aspects of the PGS. It is based on the principal that the external and internal area of government 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. This physical security goal, found in GCPSG-010 Operational Physical Security Guide, includes the concept of protection, detection, response, and recovery (PDRR).

5.1. Preventative Approach

The prevention of harm or damage is accepted as being less costly, in terms of human and financial loss, than it is to repair the damage after it occurs. This summarizes the importance of incorporating PDRR elements into GC physical security systems. Protection, Detection, and Response are interdependent elements that enable a natural recovery to normal operations in a cost and time efficient manner. Periodic tests of security procedures, plans, and equipment should be undertaken by authorized persons to verify compliance with each department or agency's security practices in order to achieve a higher preparedness level for potential security threats.

5.1.1. Crime Prevention Through Environmental Design

Crime Prevention Through Environmental Design (CPTED) is a multi-disciplinary approach to crime prevention during the designation, definition, and security design of an environment. Facility design and management of natural and man-made environments, can enable departments and agencies to deter criminal or adversarial actions while safely managing the flow of individuals throughout a facility. These models intend to positively influence behavior and activities while discouraging undesirable actions by staff, visitors, and potential adversaries.

5.1.2. Threat Risk Assessment and Risk Management

A Threat and Risk Assessment (TRA), is a process used to identify, analyse, and address observed vulnerabilities against known or anticipated threats to establish the risk environment and is an integral part of a department or agency's overall risk management strategy. Once a department or agency's risk landscape has been established, application of these PDRR concepts and other physical security guides, found at RCMP LSA Publications, will aide in managing known risks and in building resilience to rare or unforeseen risks in the future.

6. Protection

Protection is achieved through the use of physical, procedural and psychological barriers to delay or deter unauthorized access. Protection safeguards impede the occurrence of unwanted events and are often referred to as barriers. A protective barrier should serve some or all of the following functions:

- Mark the perimeter of a restricted access area or zone;
- Provide a level of protection from physical attack or force;
- Deter an intrusion by making an assailant/attacker/trespasser more readily identifiable;
- Prevent, delay, or control access by unauthorized personnel or vehicles;
- Contain personnel or assets within a room, area, or zone; and
- Impede escape.

A barrier is considered effective against unauthorized access when it restricts access routes to an asset and is able to stop or hinder the unauthorized person(s) approaching from any side. An assessment must be completed against known and likely threats, the probable adversary, and the adversary's motivation, capabilities, skill, and resources. Protection from threats identified in a TRA should include:

6.1. Physical Barriers

Physical barriers are passive, active, or a combination of the two.

A passive barrier, such as a bollard, restricts the unauthorized vehicles from passing but it will not respond to an attack.

Active barriers react or are altered when there is unauthorized activity; for example, security guards on patrol.

A combined active and passive barrier could be a fence that restricts access to the area by creating a compound perimeter which is then used to contain patrolling guards that would detect and respond to an intruder.

When detection does not activate an effective response, a physical barrier system does little more than provide a psychological barrier to a determined and skilled adversary. Without the elements of detection and response, a barrier will only deter the initiation of the event and limit unskilled opportunistic adversaries.

6.1.1. Objectives of Physical Barriers

There are usually two objectives for physical barriers:

- To make penetration so complex or difficult that only a few attackers will be able to breach the barrier, and
- To delay or if possible stop an intrusion and/or attack.

6.1.2. Complexity of the System

A well-planned design reduces the number of potential attackers who have the necessary knowledge, determination, skills and resources to overcome a barrier. Barrier designs that employ a variety of materials and procedures can help deter many potential attackers who may not be skilled or ambitious enough to take on this challenge.

6.1.3. Prolonging and Delaying Attack

A robust barrier requires time in order to exploit or defeat. Barrier time-delay design should incorporate the following characteristics:

- Amount of force required to defeat the barrier;
- Amount of time needed to defeat the barrier (delay);
- Ability to recognize any attempts to defeat the barrier; and
- Response time of the guard force / police force.

6.1.4. Layering Barriers

Security systems are often designed utilizing multiple barriers encircling a protected asset; commonly referred to as "defense-in-depth" or "rings of protection". Layered barrier designs are advantageous when they require increased knowledge, skill, and talent to circumvent and, as a result, increase the likelihood of being discovered due to a prolonged exposure of an attacker's efforts at each layer of protection. This enables detections systems to promptly identify the incident and initiate a response.

6.2. Procedural Barriers

The use of routine procedures, to establish a baseline standard of acceptable conduct or activity, will aid personnel in recognizing actions and behaviours that fall outside of the norm; which in turn supports Detection. The use of security staff, log books and administrative procedures, such as signing into an office area, can act as a deterrent to any unwanted activity. Procedures such as these can be automated which can activate a response when they are not properly followed. They may also deter unwanted activity by creating a perceived barrier to entry into an area; which tends to prevent compromise of the asset.

Example: Access to files in a file room. If administrative procedures require someone to sign out or record files accessed, this may act as a deterrent for individuals to take any files without the specific need-to-know of the file contents. Thus, protection of information in the files is achieved in accordance with the need-to-know and need-to-access principles.

6.3. Psychological Barriers

A psychological barrier is a deterrent only, as it does not hinder or stop an event if the adversary decides to attack. A psychological barrier such as the presence of CCTV cameras or functioning security lighting illuminating a facility will help to confirm to any trespasser that they will be easier to detect but it will not physically prevent anyone from entering the area. The intruder will recognize this will increase their risk of being detected and could generate a response from security personnel. The extent of usefulness of specific psychological barriers should be determined through the TRA process.

7. Detection

Detection involves the use of appropriate design, devices, systems, and procedures to signal that an attempted or actual unauthorized access has occurred. Detection systems should be designed and implemented with the intent of providing the earliest possible notification, of any event, in order to reduce the amount of time needed to provide an appropriate response. Detection elements increase the effectiveness of protection measures if employed in a complimentary manner as part of any department or agency's access management system. Additional information on access management is found in GCPSG-006 Access Management Guide.

7.1. Electronic Intrusion Detection

Electronic Intrusion Detection (EID) systems are intended to provide continuous monitoring of vital or high value locations, access control points, zones in which access is controlled (OZ, SZ, HSZ), and any other spaces in which human supervision and control is not possible. EID systems often are incorporated with alarm systems, fire safety systems, CCTV, security lighting, and electronic access control card systems. EID must be monitored by personnel capable of coordinating a response when intrusions or emergencies occur. Best practice is for departments and agencies to establish a Security Operations Centre (SOC) to lead in this function.

7.2. Security Operations Centre

A SOC provides a facility to support security personnel in the monitoring, surveillance, display, control, management and response to security-related events. A SOC typically provides 24-hour surveillance activities through video camera systems, intrusion alarm sensors, and related systems. The SOC also provides the ability to detect and assess alarm notifications and dispatch staff to address the issue such as Contracted Security teams, Commissionaires, or Emergency Services personnel. There are a number of critical functions carried out within the SOC and situational awareness is at the forefront of the operational purpose. Operators in the SOC:

- Collect information related to the controlled and monitored environment;
- Analyze the information to determine the impact to personnel or the facility;
- Respond to the situation appropriately; and
- May also be utilized to function as a command centre during emergencies.

More information concerning the functions of using a SOC are found at GCPSG-003 Security Operations Centre Design Considerations Guide.

7.3. Security Awareness Programs

As per DSM, Appendix H: Mandatory Procedures for Security Awareness and Training Control, GC departments and agencies must develop and maintain a security awareness and training program for employees at all levels. It is strongly encouraged that direction on which procedures staff must initiate when observing or experiencing security incidents is included in all security awareness programs. Developing a strong culture of security co-operation and reporting will strengthen the detection functions within GC departments and agencies.

8. Response

Response entails the implementation of measures to ensure that security incidents are being reported to appropriate security officials, and ensures that immediate and long-term corrective action is taken in a timely fashion. Response priorities, in order, are:

1. Preservation of life and safety of personnel;
2. Safeguarding of GC information and assets; and
3. Protection of property to enable prompt recovery to normal operations.

Department and agency response plans and SOP should be based upon a TRA that includes known and anticipated threats to the location and personnel, capabilities of onsite security personnel, and available support from First Responders (Police, Fire, Ambulance). These should be routinely practiced (exercised) by both security and non-security personnel in order to foster a greater preparedness and enable an agile recovery to normal operations. These exercises may include scenarios based on fire emergencies, facility evacuations, emergency destruction plans, intruder alarms, lockdowns, armed intruders, natural disasters, and protests or demonstrations. Methods available to test these plans include table-top exercises, Emergency Response Team (ERT) training, practical scenario-based training and exercises, and penetration tests.

9. Recovery

Recovery refers to the restoration of full levels of service delivery following an incident. The ability of a department or agency to recover from an incident, also referred to as resiliency, is directly enabled by the measures employed in the areas of Protection, Detection, and Response. In a physical security context, this may include:

- Delivery of an apprehended intruder to responding police;
- Returning to office spaces following a fire alarm evacuation;
- The restoration of damaged or compromised access management systems; or
- The activation of an Alternate Command Post (ACP) or Alternate Service Delivery Point (ASDP) until the original location is safe and fully operational.

Following an incident, a review of the key elements of the event, and actions taken to prevent or limit the impact, should be included in the recovery process. The lessons learned from each incident can then be incorporated into a department's or agency's PDRR preparations and plans.

10. Collaborative Application of PDRR

Developing robust protection features, comprehensive detection systems, and well-trained and exercised response services will help enable the resiliency that departments and agencies need for a swift recovery from a security incident/event; as per GC Business Continuity Management (BCM) requirements. The PGS and Federal Policy for Emergency Management identify Public Safety Canada (PS) as the Lead Security Agency for BCM. PS can provide additional information on BCM via their Centre for Resiliency and Continuity Management. Additionally, as society

embraces technological advances, PDRR for physical security and information technology (IT)/cyber security are becoming more entwined. The PGS identifies the Communications Security Establishment (CSE) as the lead technical authority for IT security. CSE can provide additional information via their Canadian Centre for Cyber Security.

When designing a PDRR system, it is important that all aspects of the system work in a complementary fashion to ensure its effectiveness. To help in identifying the necessary aspects of a PDRR system, the following should be considered:

1. What is of value or perceived value that an adversary may wish to:
    - Disclose (example: sell information to others);
    - Interrupt (example: stopping electrical power service to a facility);
    - Modify (example: change the intention of written documents or electronic files);
    - Destroy (example: burn); or
    - Remove (example: steal).

2. Who/what is the known or potential threat? Is the risk from:
    - An individual or group (client, former employee, current employee/insider threat);
    - An organization (organized crime, terror group);
    - Another nation (espionage, political or trade adversary); or
    - Environmental Risks (natural disasters, climate change, remote locations, high crime).

3. How/why a known or potential threat may impact the facility:
    - What is the known or likely method of intrusion or attack;
    - What are the known or likely capabilities of an adversary;
    - What are the known or assessed motivations of an adversary;
    - What are the stated or assessed intentions of an adversary; and
    - What is the known history of incidents occurring in the area and/or against the GC, department, or agency?

Once these considerations are investigated, assessed via a TRA, and addressed with interoperable protection barriers and measures, detection systems, and response personnel, departments and agencies can be better suited to mitigate the risk and enable timely recovery from threats to GC personnel, information, and real property.

11. Reference and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- Federal Policy for Emergency Management- Canada.ca
- Public Safety Canada - Centre for Resiliency and Continuity Management
- Canadian Centre for Cyber Security
- GCPSG-003 Security Operations Centre Design Considerations Guide

- GCPSG-006 Access Management Guide
- GCPSG-010 Operational Physical Security Guide
- International CPTED Association

12. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-019 (2023) – Protection, Detection, Response, and Recovery Guide, for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2023.12.12 14:06:21 -05'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve GCPSG-019 (2023) – Protection, Detection, Response, and Recovery Guide.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.01.05 12:31:28 -05'00'

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

Date