Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Operational Security Standard on Physical Security

Published: Feb 18, 2013

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-19/2013E-PDF
ISBN: 978-0-660-09869-2

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Norme opérationnelle sur la sécurité matérielle

Operational Security Standard on Physical Security

1. Preamble

In accordance with the Policy on Government Security and Appendix C of the Directive on Departmental Security Management, this standard provides baseline physical security requirements to counter threats to government employees, assets and service delivery and to provide consistent safeguarding for the Government of Canada. The standard contains both requirements (indicated by use of the word “must” in sentences appearing in italics) and recommended safeguards (indicated by the use of the word “should”).

Baseline levels are designed for common types of threats that departments would encounter. Certain departments or operations may face different threats because of the nature of their operations, their location and/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 and other assets information apply to both government and non-government facilities.

2. Definitions

Refer to Appendix A for definitions.

3. Roles and Responsibilities

All departments are responsible for safeguarding employees, assets and service delivery within their area of responsibility.

3.1 Tenant Department Responsibilities

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.)

3.2 Custodian Department Responsibilities

Custodian departments are responsible for providing and funding safeguards considered necessary by the custodian to protect facilities, based on a threat and risk assessment conducted by or for the custodian. This responsibility includes implementing and integrating measures for base building security (e.g., exterior doors and lighting), building systems (e.g., elevator, mechanical and electrical systems) and life safety (e.g., exit stairs, fire alarms and sprinklers). Custodians are also responsible for integrating tenant-funded requirements, both baseline and enhanced, into their base building infrastructure.

4. Other Treasury Board Policies and Operational Security Standards

This standard is complemented by other operational security standards found at the Treasury Board Security Policy Web site and by technical documents on physical security produced by the RCMP.

The provisions of this standard complement the Treasury Board policies on real property - Policies and Publications and occupational safety and health - Policies and Publications.

5. Types of Threats Conditions

The following threats are common to all government departments. 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 are not immune from oral or written threats or acts of physical violence (e.g., assault as defined in the Criminal Code, intimidation and stalking) by other employees or members of the public. Work related threats can occur at the workplace or outside the workplace while employees are on duty or in some circumstances, off duty.

The Canada Labour Code recognizes the problem of violence and requires that employees be appropriately protected. The employer (the Government of Canada) recognizes the need for employees to be free, to the greatest extent possible, of intimidation so that they can safely perform their mandated functions. The pending 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. The Regulations, once promulgated, must be followed when establishing procedures.

For further information refer to Appendix C-Security Control Objectives of the Directive on Departmental Security Management.

5.2 Unauthorized Disclosure of Protected and Classified Information

Unauthorized disclosure of protected or classified information can occur:

a. accidentally through loss or negligence by employees who were granted access to the information;
b. intentionally by individuals who have authorized (i.e., have been properly security screened and have a need to know) access to the information; and
c. intentionally by individuals who gain unauthorized access to information by whatever means, e.g., 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 and maintenance of the economic, social or political stability of Canada, compromise of other governments' interests, breach of privacy, liability or financial loss, loss of confidence in the Government of Canada, 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 delineated for this level of information.

5.3 Unavailability of Assets, and Monetary or Heritage Loss

Theft, fraud, vandalism, cyber attack and “malicious activity”, accidental or intentional loss or damage by employees or members of the public, and natural events (such as 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 to the functioning of 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 their intended use. The result is that Canadians could make wrong decisions and damage their economic or social circumstances. The impact also includes liability, financial loss, loss of confidence in government, and temporary or prolonged inability to govern properly. The injury increases with the importance of the information or other asset to Canadians and the government e.g., cheque producing equipment).

6. Physical Security Approach

The government's approach to physical security complements other aspects of the Policy on Government Security (PGS) and is based on the theory that the external and internal environments of facilities can be designed and managed to create conditions that, together with specific physical security safeguards, will reduce the risk of violence to employees, protect against unauthorized access, detect attempted or actual unauthorized access and activate an effective response.

Physical security strategies are based on (1) the concept of protection, detection, response, and recovery; (2) design based on a series of clearly discernable zones; (3) control of access to restricted areas; and (4) the capability to increase security during emergencies and increased threat situations.

6.1 Protection, Detection, Response and Recovery

Departments must ensure that their physical security strategy incorporates identifiable elements of protection, detection, response and recovery.

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

Refer toRCMP Guide G1-025, Protection, Detection and Response, for more information.

With regards to recovery, refer to the Operational Security Standard - Business Continuity Planning Program.

6.2 Hierarchy of Zones

Departments must ensure that access to, and safeguards for, protected and classified assets are based on a clearly discernable hierarchy of zones. There are five zones:

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

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 where initial contact between visitors and the department occurs; this can include such spaces as places where services are provided and information is exchanged. Access by visitors may be limited to specific times

of the day or for specific reasons.

Operations Zone
: is an area where access is limited to personnel who work there and to properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored periodically. Examples: typical open office space, or typical electrical room.

Security Zone
: is an area to which access is limited to authorized personnel and to authorized and properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously, i.e., 24 hours a day and 7 days a week. Example: an area where secret information is processed or stored.

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, i.e., 24 hours a day and 7 days a week and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel.

The last three zones, operations, security, and high security are referred to as restricted-access areas.

Instituting a hierarchy of zones allows departments to:

a. Store assets of different threat levels in the same facility,
b. Institute varied levels of controls of access to protect various levels in assets,
c. Reduce cost by processing and destroying various levels of information and assets within the same facility, and
d. With appropriate planning, change zones from one period of time (working hours) (eg. Operations zone) to another period of time (silent hours) (eg. Security zone).

Access to the zones should be based on the concept of "need to know" and restricting access to protect employees and valuable assets. Refer to RCMP Guide G1-026, Guide to the Application of Physical Security Zones for more detailed information.

The appropriate number of zones within a facility is dependent on 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 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 must control access to restricted-access areas using safeguards that will grant access only to authorized personnel.

Control of access to restricted-access areas and other departmental space must be provided in a manner which 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). Refer to RCMP Guide G1-010 - Security Connotations of the 1995 National Building Code, for more information on typical National Building Code security related issues.

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 may also consider electronic access control (e.g., card access, PIN access or biometric access control) to meet the requirement for mandatory control of access. A threat and risk assessment will determine the appropriate cost effective means to control access to a facility.

To facilitate the proper control of access to departmental space, departments must carefully plan, using the TRA methodology, how individuals and material will enter their space.

Departments 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 threat and risk assessment

For more detailed information see the RCMP Guide G1-024 Control of Access.

6.4 Capability to Increase Security in Emergency and Increased Threat Situations

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. For more information refer to the Operational Security Standard - Readiness Levels for Federal Government Facilities.

7. Security in the Selection and Design of Facilities

7.1 Introduction

Departments must review their existing facilities as part of their threat and risk assessment activity to determine whether remedial measures are needed.

The requirements of this operational standard are neither specific to a particular type of facility nor all-encompassing. While they are typical of office buildings, they apply to other facility types (such as warehouses, laboratories, lands, bridges, wharves and dams) that may require unique safeguards to provide adequate security against the threats identified in this standard.

The Policy on Government Security and Appendix C-Security Control Objective of the Directive on Departmental Security Management require departments to ensure that security is fully integrated early in the process of planning, selecting, designing and modifying their facilities. It is important to ensure that security is thoroughly addressed in all phases of a construction or modification 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 threat and risk assessment. Departments must include the necessary security specifications in all plans, request for proposals and tender documentation for construction or modification projects and incorporate related costs in funding requirements.

The following information is intended for use by project managers and real property and security professionals in establishing a safeguarding strategy for a particular project.

7.2 General Security and Planning

7.2.1 Applicable Codes and Policies

Departments must ensure that physical security measures comply with applicable regulations, codes and policies. Examples include labour, fire, building and electrical regulations and codes and Treasury Board real property policies.

7.2.2 Emergency Power

Emergency power must be provided for base building services (e.g., partial elevator service and emergency lighting) to the extent appropriate for departmental facilities in order to facilitate safe evacuation in the event of an emergency and to protect government assets. A threat and risk assessment will determine the emergency power requirements for security systems (e.g., electronic door locks, CCTV, alarms). As a minimum, the emergency power must be provided in conformance with 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 should 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 tenant's facility, employees or equipment.

7.3.2 Control of Site Perimeter

Control of the site perimeter should be achieved through the application of crime prevention through environmental design principles. Examples include keeping intruders under observation through natural surveillance, decreasing crime opportunities through natural access control and creating a sense of ownership through territorial reinforcement as well as such landscape features as fences, planters and site grading.

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 (e.g., from nearby roadways or other buildings) unless this approach is deemed undesirable by departmental safeguarding strategies. Departments 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

Fire water capacity and the effective response times of firefighters and police should be taken into account during the development of safeguarding strategies (based on protection, detection and response) that apply to site selection, facilities and assets. For example, alternative measures for life safety and asset protection may be required to compensate for inadequate emergency response times. Departments must seek and follow the direction of the FFPA with respect to the water supply requirements for fire fighting.

7.3.5 Adjacent Occupants and Use

Consideration should be given to adjacent occupants and use during site selection, including 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 (e.g., vandalism and work-related violence) and support surveillance features (e.g., natural surveillance and closed-circuit video systems). The choice of light levels should be based on applicable codes, camera technology and other security considerations. Refer to RCMP Guide G1-002 - Security Lighting for more information.

7.3.7 Exterior Signs

Where signs identify facilities occupied by federal government departments and agencies they must comply with the Federal Identity Program. In addition, facilities should display signs that give clear directions for parking, visitors, employees and service areas. Consideration should be given to the conditions imposed by provincial or territorial law to prove trespass when signs are used to define the boundaries of government property or establish restricted-access areas in accordance with a TRA.

7.3.8 Landscape Design

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

- clearly marked boundaries;
- circulation routes designed to promote natural surveillance;
- no cover for intruders;
- unobstructed views for security personnel, employees and the public of potential problem areas (e.g., where criminal activities might occur); and
- avoidance of materials and furniture that might expose the facility to increased risk during a heightened state of security (e.g., if a demonstration turns violent).

Landscape design should apply the principle of crime prevention through environmental design principles. Examples include keeping intruders under observation through natural surveillance, decreasing crime opportunities through natural access control and creating a sense of ownership through territorial reinforcement as well as such landscape features as fences, planters and site grading.

7.3.9 Parking

The threat and risk assessment will determine the needed safeguards to protect employees in parking areas. Such safeguards may include putting a designated parking area close to the facility, adequate lighting, or a buddy system whereby employees can be 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 and life safety measures as well as 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 (such as 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 Circulation Corridors and Elevator Lobbies

Circulation routes which provide employees and visitors access to restricted-access areas must be carefully planned to

ensure life safety requirements are met as well as to ensure that access is controlled to areas where valuable, protected and classified assets are stored.

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 having a High Security zone located on a particular floor such as a cross-over floor in a high rise building could require in the event of an emergency that public pass through the High security zone to gain access to a second stairwell. Other areas which require a balance between life safety and physical security concerns include elevator lobbies, corridors, and hardware limitations. RCMP Guide G1-024 - Control of Access, Appendix A provides Best Practices related to zoning and building layout, compartmentalization, cross over floors, access to exits etc.

Access by employees and visitors to restricted-access areas should be based on the principle of need to know with consideration of overviewing and overhearing.

The circulation routes followed by employees to transport valuable assets should be planned in a way that addresses the threats identified through a 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, a reception function, or procedures such as limiting elevator use to authorized personnel or having employees challenge people.

7.5.2 Daycare Centres

When daycare centres are planned for federal facilities, consideration must be given to the safety of both the tenants and the public in the context of the Government of Canada's responsibilities and liability. Daycare centres should not be co-located with departments whose programs or operations may be subject to interruption or increased threats due to events such as demonstrations, or with departments that might deal with high-risk clients (including potentially violent individuals).

7.5.3 Stairwells and Elevators

Stairwells and elevators should not provide direct access to the tenant's restricted-access areas or to the custodian's critical facility infrastructure. Where possible, passenger and freight elevators (including those from parking and loading dock areas) should open into a Public or Reception Zone, such as the ground floor elevator lobby. However, elevators may open into tenant space, and exit stairwells may allow entry to the 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 (as per Section 5.1) must be considered in regard to the location of employee and public washrooms. When recommended by a TRA, employee washrooms should not be accessible from public or reception zones.

7.5.5 Amenity Spaces

Consideration must be given to employee safety during the design and layout of common amenity spaces (such as gymnasiums, food service areas, common meeting rooms or conference facilities). It should not be necessary for personnel to enter a department's restricted zone 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 Treasury Board's Information Technology Standard 6.9: Canadian Open Systems Application Criteria (COSAC), Telecommunications wiring system in Government-Owned and leased buildings - Implementation Criteria.

7.6 Controlling Restricted-Access Areas

Departments have several choices available to control access to restricted-access areas: personal recognition, access badges, mechanical measures, electronic control of access, etc. The appropriate choice will depend on the location of building, number of employees, threat and risk assessment etc. Refer to RCMP Guide G1-024 Control of Access, for more information on methods to Control access.

7.6.1 Identification Cards

All government employees **must be** issued an identification (ID) card, which as a minimum includes the name of the department, the bearer's name and photo, a unique card number and an expiry date. A signature is recommended. Refer to RCMP Guide G1-006 Identification cards/Access badges, for more information

7.6.2 Access Badges

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. Refer to RCMP Guide G1-006 Identification cards/Access badges, for more information.

7.6.3 Electronic Access Control

An electronic access control is a safeguard that will assist in controlling access to a facility. A threat and risk assessment will assist in determining the need and cost effectiveness of such a system. Sometimes when a department chooses to implement an electronic access control system, the requirements for an ID card and an access badge are combined in one electronic access control card.

7.6.4 Closed Circuit Video Equipment (CCVE)

Closed circuit video surveillance/assessment equipment may assist a department in providing appropriate monitoring of access to their facility. A threat and risk assessment will assist in determining the need for CCVE.

7.6.5 Security Control Centre

A security control centre, 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 closed circuit video equipment. This centre will typically include other personal or life safety equipment such as the fire alarm panel. A control centre of this nature would typically only be used in the larger facilities.

7.6.6 Sensitive discussion areas

A sensitive discussion area (SDA) is an area that is specially 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 should carefully assess the need, the risk and cost-effectiveness of options. When construction and use of an SDA is being considered, the RCMP should be consulted on needs definition, options, construction standards and procedures for the proper administration of the SDA.

For further information, see the RCMP Guide G1-004 - Construction of a Special Discussion Area.

7.6.7 Secure rooms

Secure rooms are rooms constructed according to technical standards for the storage of Protected and Classified information and assets.

Classified and Protected information stored in the appropriate type of secure room need not be further protected by storage in additional security containers, unless the application of the need-to-access principle is still a concern. A records office where protected and classified information is stored on open shelves must be constructed as a secure room. For further information see the RCMP Guide G1-029 - Secure Rooms for construction specifications for SR-1 (low security) and SR-2 (high security) respectively.

7.6.8 Security Guards

If a TRA identifies a security requirement that necessitates a human function, then employing guards in that situation is appropriate. In this case various issues related to guard type (proprietary or contract), duties, training, equipment and safety, should be addressed. For additional recommendations regarding guard services, refer to RCMP Guide G1-008 - Guidelines for Guard Services.

7.7 Facility Management

7.7.1 Leases and Other Occupancy Agreements

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

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.

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 organized for the facility. The locks on perimeter doors should be keyed separately from other locks, and they should not enable access with a master key.

Keys for the entire facility, spare keys and the information needed to reproduce keys must not all be stored in the same container. Master keys should not leave the building. Security and High Security Zones should not be part of the master keying system.

Refer to RCMP Guides G1-016, G1-017 and G1-018 for more information on Hardware, Doors and Frames, and Master Key Systems respectively.

7.7.5 Renovation Work

Where renovation work needs to be done within restricted zones, there should be advance consultation between the security and real property officials of custodian and tenant departments on security arrangements for access by contractor personnel.

7.7.6 Facility Security Committee

In multi-tenant facilities, a security committee chaired by major tenant or the custodian should be organized to coordinate the custodian's and tenants' requirements for control of access and to plan 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 must be stored in approved containers and restricted-access areas as per the minimum requirements laid out in Appendix B.

Protected and classified assets, (e.g., classified research and development equipment, engineering models or prototypes) must be stored in containers approved for that purpose as listed in the RCMP Guide G1-001 - Security Equipment Guide. For requirements not met by items listed in the Security Equipment Guide, contact the RCMP Technical Security Branch.

Care needs to be taken to ensure that classified and protected information and valuable assets (e.g., laptops) are properly safeguarded when occupants are away from their workstations for any length of time.

8.2 Security Containers

When different levels of protected or classified assets are stored together, storage should comply with the standard set for the most sensitive asset involved. The infrequent storage of a relatively small amount of assets having high-level sensitivity with a larger amount of assets with a low-level sensitivity may not warrant enhanced safeguards; refer to Appendix B.

Classified information should not be stored with valuable assets such as cash or drugs in the same security container.

Brief cases are not considered storage containers and should not to be used as such. Refer to Section 9 Transport and Transmittal.

Departments must develop procedures for the storage of assets shared with the Government of Canada, other Canadian governments, foreign governments, international, educational and private sector organizations. Procedures must be in accordance with agreements or arrangements between the parties concerned and the GSP.

All employees working off site must safeguard information as per the minimum requirements outlined in Appendix B. Employees should also consult the TB Policy on Telework. With respect to off-site contract work, departments should use the Security Requirements Checklist (TBS/SCT 350-103) to define the contract requirements for safeguarding protected or classified assets at the contractor's facilities.

8.3 Valuable Assets

Valuable assets must be afforded protection against loss, destruction or alteration. The degree of protection afforded is dependant on 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's Technical Security Branch.

8.4 Keys for Security containers

Keys in this section include mechanical keys, combinations, personal identification numbers, and access cards.

Keys for security containers must be safeguarded commensurate with the highest sensitivity 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 must be changed when (1) there is evidence of compromise, (2) a threat and risk assessment indicates an unacceptable level of risk, or (3) an employee's need to access the security container has changed. Combinations to security containers should be changed every year.

A record of all changes to keys for security containers must be kept, including: the date, reason, custodian, location and, if applicable, lock identifier, combination number, duplicates, etc. This record of change must 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 are responsible for the disposal of security containers. Approved security containers for Protected C and classified information must not be disposed of or resold to private sector or outside agencies. Refer to RCMP Guide 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 must ensure that approved storage equipment is properly serviced and maintained at all times. Refer to RCMP Guide G1-001 - Security Equipment Guide and related News/Bulletins for more information.

9. Transport and Transmittal

Maintaining authorized access to protected and classified assets and valuables is paramount when being transported.

1. 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.
2. When transmitting protected and classified assets from one person or place to another, safeguards must depend on proper packaging, an appropriate and reliable postal or courier service (government or private sector) and the anonymity of the information while in transit.
3. For the limited amount of protected and classified assets that are at higher risk, appropriate additional safeguards should be used, as indicated in the TRA.
4. Departments must transport or transmit protected and classified assets according to the minimum requirements set out in Appendix C.
5. Refer to RCMP Guide G1-009 - Transport and Transmittal of Sensitive Information and Assets for detailed specifications for enveloping, addressing and courier services for transporting and transmitting protected and classified assets.
6. Departments are responsible for safeguarding security equipment (for example, security containers) during transport for servicing requirements.

10. Destruction

10.1 Storage of Protected and Classified Waste

Protected and classified assets awaiting destruction (either on- or off-site) must be stored at minimum in approved security containers or appropriate secure room as per Appendix B. Departments must safeguard information in transit to destruction, in the manner prescribed for the highest level of classified or protected information involved (refer to RCMP Guide G1-009 - Transport and Transmittal of Sensitive Information and Assets).

10.2 Destruction of Assets

Departments 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.

Protected and classified information with no historical or archival value for which the retention period have expired, must be promptly destroyed including surplus copies, draft copies and waste.

Protected and classified information must be destroyed using equipment listed in the RCMP Guide G1-001 - Security Equipment Guide. For requirements not met by items listed in the Security Equipment Guide, contact the RCMP Technical Security Branch.

When a department is responsible, on behalf of another department, for transporting protected and classified information to destruction, or for destroying such information, written authorization of destruction must be obtained.

Protected and classified information must not be disposed of through a federal or municipal recycling program unless properly destroyed in an approved manner prior to recycling.

The destruction of information must be performed by individuals in the department who are appropriately security screened to the highest level of protected or classified information being destroyed.

Departments must ensure that anyone who performs shredding is security screened commensurate with the highest level of information being destroyed. Departments are also responsible for ensuring that the shredded material conforms to the size standards noted in RCMP Guide G1-001 - Security Equipment Guide.

10.3 Electronic Storage Media

For guidance on the disposal and destruction of electronic storage media see the Communications Security Establishment Canada (CSEC) Information Technology Security Guideline (ITSG-06) - Clearing and Declassifying Electronic Data Storage Devices.

10.4 Emergency Destruction Abroad

In situations abroad where the likelihood of emergency destruction is high, there must be local orders for the prompt destruction of Top Secret and Secret information when its secure transport or transmittal to Canada 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. Enquiries

Enquiries about this policy should be directed to the Departmental Security Officer. For interpretation of the standard, the Departmental Security Officer should contact the Security and Identity Management Division.

Appendix A - Definitions

For the purposes of this standard the following definitions apply.

assets (biens)
: 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.

attack (attaque)
: any action to execute a threat.

availability(disponibilité)
: the condition of being usable on demand to support operations, programs and services.

base building security (sécurité de l'immeuble de base)
: Security safeguards provided by the custodian department to protect a facility but not the assets contained in the building. Basic building security provides a base or starting point for other security requirements (i.e. minimum and enhanced safeguards) to be added to protect the specific assets held by the institution.

baseline security requirements (exigences de base)
: mandatory provisions of the Policy on Government Security and its associated operational standards and technical documentation.

business continuity planning (planification de la continuité des activités)
: an all-encompassing term which includes the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets.

classified assets (biens classifiés)
: assets whose compromise would reasonably be expected to cause injury to the national interest.

classified information (renseignements classifiés)
: information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest.

compromise (compromission)
: unauthorized disclosure, destruction, removal, modification, interruption or use of assets.

control of access (contrôle de l'accès)
: 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 department (ministère gardien)
: a department having administration of federal real property.

department (ministère)
: as described in Section 2: Application, of the PGS. In this document the term “department” may refer to either the tenant, the

custodian or both.

destruction equipment (équipement de destruction)
: any device or process used to change the medium which contains classified or protected information in such a way that the classified or protected information can no longer be derived from the medium.

detection (détection)
: the use of appropriate devices, systems and procedures to signal that an attempted or actual unauthorized access has occurred.

facility (installation)
: a physical setting used to serve a specific purpose. A facility may be part of a building, a whole building, or a building plus its site; or it may be a construction that is not a building. The term encompasses both the physical object and its use (for example, weapons ranges, agriculture fields).

information (renseignements)
: any pattern of symbols or sounds to which meaning may be assigned.

integrity (intégrité)
: the accuracy and completeness of assets, and the authenticity of transactions.

material (matériel)
: any tangible object with the exclusion of those embodying information.

monitored (surveillé)
: To watch for or detect a breach of security.

monitored continously (surveillée continuellement)
: To confirm on a continuous basis that there has not been a breach of security. Examples include electronic intrusion detection system, or someone guarding a particular point on a constant basis.

monitored periodically (surveillée sur une base périodique)
: To confirm on a regular basis that there has not been a breach of security. The frequency and diligence of monitoring is based on the recommendations of a Threat and Risk Assessment. Examples include a guard patrol, or employees working at the location.

national interest (intérêt national)
: Concerns the defence and maintenance of the social, political and economic stability of Canada.

need-to-know (besoin de connaître)
: The need for someone to access and know information in order to perform his or her duties.

personnel security screening (enquêtes de sécurité du personnel)
: the process of examining the trustworthiness and suitability of employees and, where national interest is concerned, their loyalty and associated reliability. When satisfactory, an employee is granted reliability status or a security clearance. Reliability status applies when only protected assets are concerned. When the employee has access to classified assets, a security clearance corresponding to the level of classified assets is issued. A security clearance includes reliability status. See Screening.

physical security (sécurité matérielle)
: the use of physical safeguards to prevent or delay unauthorized access to assets, to detect attempted and actual unauthorized access and to activate appropriate responses.

protection (protection)
: for physical security, protection means the use of physical, procedural and psychological barriers to delay or deter unauthorized access, including visual and acoustic barriers.

protected information (renseignements protégés)
: information related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to a non-national interest.

protected and classified information (renseignements protégés et classifiés)
: See Protected Information and Classified Information.

recovery (rétablissement)
: to the restoration of full levels of service delivery.

response (intervention)
: the implementation of measures to ensure that security incidents are reported to appropriate security officials and immediate and long-term corrective action taken.

restricted - access area (zone d'accès restreint)
: work areas where access is limited to authorized individuals includes Operations, Security and High Security Zones. Refer to the definition in Section 6.3. Hierarchy of Zones.

risk (risque)
: the chance of a vulnerability being exploited.

security container (coffre de sécurité)
: any totally enclosed storage place for a classified asset, designed to resist force and surreptitious attacks; e.g., a safe, security cabinet, strongbox, permanent vault, demountable vault or secure room.

screening (triage)
: the process of verifying visitors and/or material (e.g. incoming mail/deliveries) at entry points of a facility or a restricted area for authorizing access; See Personnel Security Screening.

shredding (déchiquetage)
: a mechanical cutting or grinding method of reducing standard weighs of office paper, microfilm and microfiche to fragments.

surreptitious attack (attaque subreptice)
: a secret unauthorized attack to breach or circumvent a defensive system or some of its components in such a manner that the custodians and/or security force cannot readily detect the attack.

tenant department (ministère locataire)
: a department occupying federal real property that is under the administration of another department or Crown Corporation.

threat (menace

Any potential event or act, deliberate or accidental, that could cause injury to employees or assets.

unauthorized access (accès non autorisé)

Access to assets by an individual who is not properly security screened and/or does not have a need-to-know.

unauthorized disclosure (divulgation non autorisée)

Disclosure that is forbidden by law or by governmental or departmental policies.

value (valeur)

estimated worth: monetary, cultural or other.

vulnerability (vulnérabilité)

an inadequacy related to security that could permit a threat to cause injury.

zones (zones)

A series of clearly discernible spaces to progressively control access

Appendix B - Minimum Safeguards for Protected and Classified Assets

Activities	Protected A	Protected B	Protected C	Confidential	Secret	Top Secret
Personnel Security Screening	**Refer to Personnel Security Screening Standard**					
Storage	Operations Zone: Lock up the information	Operations Zone: Lock up the information or if recommended by a TRA, select appropriate equipment from RCMP Guide G1-001, Security Equipment Guide	Security Zone: Select appropriate container from RCMP Guide G1-001, Security Equipment Guide	Operations Zone: Select appropriate container from RCMP Guide G1-001, Security Equipment Guide	Security Zone: Select appropriate container from RCMP Guide G1-001, Security Equipment Guide	
Mailing in Canada	**Refer to Appendix C and RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets**					
Paper Destruction	Commercially available paper shredder producing a strip-cut to a maximum width of 3/8" (10mm) or transfer to National Archives for Destruction.	Commercially available paper shredder producing a strip-cut to a maximum width of 3/8" (10mm) or if recommended by a TRA, select appropriate equipment from G1-001 or transfer to National Archives for Destruction	Select appropriate equipment from RCMP Guide G1-001, Security Equipment Guide, or transfer to National Archives for Destruction			
Facsimile Transmission	Ensure receiving fax machine is within an operations zone.		Ensure receiving fax machine is within a Security Zone, both devices are secure faxes and zone users and occupants have the same need-to-know as the recipient or the recipient is present to receive.	Ensure receiving fax machine is within an Operations Zone, and both devices are secure faxes.	Ensure receiving fax machine is within a Security Zone, both devices are secure faxes and zone users and occupants have the same need-to-know as the recipient or the recipient is present to receive.	

Appendix C - Minimum Safeguards for the Transport and Transmittal of Protected and Classified Assets

Activities	Protected A	Protected B	Protected C	Confidential	Secret	Top Secret
Transport in Canada within restricted access area	Transport Discretely		Single sealed envelope[table 2 note 1] with no security markings	Transport Discretely		Single sealed envelope[table 2 note 1] with no security markings
Transport in Canada Outside restricted access	Single sealed envelope[table 2 note 1] with no security markings appropriately addressed		Single sealed envelope[table 2 note 1] with security markings enclosed in a second secure enclosure (eg. locked brief case).	Single sealed envelope[table 2 note 1] with no security markings appropriately addressed		Single sealed envelope[table 2 note 1] with security markings enclosed in a second secure enclosure (eg. locked brief case)

area				locked brief case)
Transport outside Canada within restricted access area	Transport Discretely. Envelope not required	Single sealed envelope[table 2 note 1] with no security markings appropriately addressed		
Transport outside Canada Outside restricted access area	Single sealed envelope[table 2 note 1] with no security markings appropriately addressed	Double sealed envelope. Security mark the inner envelope and appropriately address	Single sealed envelope[table 2 note 1] with no security markings appropriately addressed	Double sealed envelope. Security mark the inner envelope and appropriately address
Transmit in Canada within restricted access area	Proprietary mail, messenger service or Departmental employee in a Single sealed envelope[table 2 note 1] with no security markings appropriately addressed			
Transmit in Canada outside restricted access area	Proprietary mail, messenger service, Departmental employee or communication letter mail (formerly first class mail) packaged in a Single sealed envelope[table 2 note 1] with no security markings appropriately addressed, or a Reliable Courier Service[table 2 note 2] or similar postal service with record of transit and delivery, packaged as for communication letter mail. Use this method only if delivery is urgent.	Proprietary mail, messenger service, or Departmental employee in a Double Sealed Envelope[table 2 note 6] with inner package security marked and appropriately addressed, or registered mail, in a Double Sealed Envelope[table 2 note 6] with inner package security marked and appropriately addressed, or a Reliable Courier Service[table 2 note 2] or similar postal service Double Sealed Envelope[table 2 note 6] with inner package security marked and appropriately addressed with record of transit and delivery, packaged as for registered mail. Use this method only if delivery is urgent.	Proprietary mail, messenger service, Departmental employee or communication letter mail (formerly first class mail) packaged in a Single sealed envelope[table 2 note 1] with no security markings appropriately addressed, or a Reliable Courier Service[table 2 note 2] or similar postal service with record of transit and delivery, packaged as for communication letter mail. Use this method only if delivery is urgent.	Proprietary mail, messenger service, or Departmental employee in a Double Sealed Envelope[table 2 note 6] with inner package security marked and appropriately addressed, or registered mail, in a Double Sealed Envelope[table 2 note 6] with inner package security marked and appropriately addressed, or a Reliable Courier Service[table 2 note 2] or similar postal service Double Sealed Envelope[table 2 note 6] with inner package security marked and appropriately addressed with record of transit and delivery, packaged as for registered mail. Use this method only if delivery is urgent.
Transmit outside Canada within restricted access area	In a Single sealed envelope[table 2 note 1] with no security markings appropriately addressed.	Proprietary mail, messenger service, or Departmental employee in a Single sealed envelope[table 2 note 1] with no security markings appropriately addressed		
	Single sealed envelope[table 2 note 1] with no security markings	Appropriately Screened[table 2 note 5] proprietary mail, messenger service Double	Appropriately Screened[table 2 note 5] proprietary mail, messenger service packaged in a Single sealed envelope[table 2 note 1] with no security	Appropriately Screened[table 2 note 5] proprietary mail, messenger service Double

Transmit outside Canada outside restricted access area	appropriately addressed and transmitted by, Proprietary mail, messenger service, or Departmental employee or communications letter mail, or a Reliable Courier Service[table 2 note 2] or similar postal service with record of transit and delivery, packaged as for registered mail. Use this method only if delivery is urgent.	Sealed Envelope[table 2 note 6] with a SIARN[table 2 note 3] placed in the inner envelope. Security mark the inner envelope and seal with approved tape, or DFAIT mail service Double Sealed Envelope[table 2 note 6] with a SAIRN placed in the inner envelope. Security mark the inner envelope and seal with approved tape.	markings appropriately addressed, or a Reliable Courier Service[table 2 note 2] or similar postal service with record of transit and delivery, packaged in a Single sealed envelope[table 2 note 1] with no security markings appropriately addressed, or DFAIT mail service Double Sealed Envelope[table 2 note 6] with inner package security marked and appropriately addressed.	Sealed Envelope[table 2 note 6] with a SIARN[table 2 note 3] placed in the inner envelope. Security mark the inner envelope and seal with Approved Tape[table 2 note 4], or DFAIT mail service Double Sealed Envelope[table 2 note 6] with a SAIRN placed in the inner envelope. Security mark the inner envelope and seal with approved tape.

Table 2 Notes

Table 2 Note 1

Single sealed envelope: A briefcase or other container of equal or greater strength, locked or sealed, can replace a single sealed envelope.

Return to table 2 note 1 referrer

Table 2 Note 2

Reliable Courier Service: The reliability of a courier service must be established through verification with other clients, or the Better Business Bureau, or the local police.

Return to table 2 note 2 referrer

Table 2 Note 3

SIARN: Sensitive Information and Assets Receipt Notification.

Return to table 2 note 3 referrer

Table 2 Note 4

Approved Tape: Refer to PWGSC Security Equipment Catalogue or RCMP Guide G1-001 - Security Equipment Guide, to obtain information on the approved security tape.

Return to table 2 note 4 referrer

Table 2 Note 5

Appropriately Screened Service: Personnel of the service are security screened to a level commensurate with the information or assets they control. See RCMP Guide G1-009 - Transport and Transmittal of Sensitive Information and Assets, for mailing procedures if personnel are not appropriately screened.

Return to table 2 note 5 referrer

Table 2 Note 6

Double Sealed Envelope: When proprietary mail or messenger service is used, the outer envelope can be replaced by a briefcase or other container of equal or greater strength, locked or sealed. Additional measures may also apply such as when involving bulk shipment. See RCMP Guide G1-009 - Transport and Transmittal of Sensitive Information and Assets.

Return to table 2 note 6 referrer