Security Inspections Guide
GCPSG-005 (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: 2023-08-09
Updated:

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Foreword

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

This is a Government of Canada publication to serve as a guide for addressing the requirements to assist in the performance of security inspections for departments, agencies and employees of the Government of Canada.

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

Reproduction

Effective Date

The effective date of GCPSG-005 Security Inspections Guide is 2023-08-09

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

1.1. Purpose

The purpose of this document is to provide Government of Canada (GC) employees with guidance on performing security inspections. Security inspections are a process whereby security personnel conduct an examination of a workplace (i.e. common work areas, employee offices or workstations) to ensure that sensitive and valuable information and assets are properly safeguarded when individuals are absent from their workspace. Performing security inspections ensures employees are abiding by established departmental and GC policies and procedures to safeguard protected and classified material stored at GC facilities. Security inspections are a critical component of a robust physical security program; they help to maintain high security standards and support the efficient, effective and accountable management of sensitive information and assets within the organization.

This guide has been developed to reflect requirements of the Policy on Government Security (PGS) and Appendix C of the Directive on Security Management (DSM). In accordance with the PGS, GC departments and agencies are responsible for the protection of information, individuals, and assets under their control, and assuring continuity of operations. GC employees have the responsibility to safeguard all GC information and assets from unauthorized access, loss, theft or disclosure. To help achieve this, periodic security inspections should be conducted to ensure this material is secured in accordance with the DSM. This guide references baseline requirements and provides guidance on security best practices. 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.

1.2. Applicability

This guide applies to GC facilities, especially to areas where protected and classified material is stored and processed. The intended audience of this guide includes:

- Directors, managers, and supervisors who are responsible for physical security zones where sensitive information is processed;
- GC authorized individuals who work or who have access to a physical security zone where sensitive information is processed; and
- GC authorized individuals who have been appointed to take on the duties of the security inspector.

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
COMCO	Communications Intelligence Control Officer
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CSO	Chief Security Officer
DSM	Directive on Security Management
GC	Government of Canada
PCO	Privy Council Office
PGS	Policy on Government Security
RCMP LSA	RCMP Lead Security Agency for Physical Security
SA&A	Security Assessment and Authorization
SCoE	Security Centre of Excellence
SIGINT	Signals Intelligence
TBS	Treasury Board Secretariat of Canada
TRA	Threat and Risk Assessment

4. Glossary

Term	Definition
Assets	Tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms, 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.
Breach	An act or omission, deliberate or accidental, that does result in the actual or possible compromise of Classified or Protected information or assets
Classified Information	Information whose compromise would reasonably be expected to cause injury to the national interest.
Compromise	A breach of government security. Includes but is not limited to unauthorized access to, disclosure, modification, use, interruption, removal, or destruction of sensitive information or assets, causing a loss of confidentiality, integrity, availability or value, any action, conduct, threat or gesture of a person toward an employee in the workplace or an individual within federal facilities that caused harm or injury to that employee or individual, and/or an event causing a loss of integrity or availability of government services or activities.
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.
High Security Zone	An area to which access is limited to authorized, appropriately security screened personnel and to authorized escorted visitors.
Need-to-access	The principle that there is a need for an authorized individual, granted an equivalent GC Security Clearance, to access a facility or zone in order to perform his or her 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	The principle that there is a need for someone to access and know information in order to perform their duties.
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 Information	Information, whose compromise would reasonably be expected to cause injury to other than the national interest.
Security Assessment	Ongoing process of evaluating security practices and controls to establish the extent to which they are implemented correctly, operating as intended, and achieving the desired outcome with respect to meeting defined organizational security requirements.
Security Container	A completely enclosed storage area for sensitive information and assets, designed to resist force and surreptitious attacks; e.g. a safe, security cabinet, strongbox, permanent vault, demountable vault or secure room.
Security Infraction	A reported instance of non-compliance with departmental policy and/or an employee's failure to comply with policy or an established guideline that may result in a security concern or risk
Security Inspection	An examination of the workplace (e.g. common work areas, an employee's office or workstation, etc.) to ensure that sensitive and

	valuable information and assets are properly safeguarded when unattended.
Security Inspection Team	A group of at least two authorized Security Inspectors who conduct security inspections.
Security Inspector	An individual delegated by the Manager(s) to be a member of the Security Inspection Team.
Security Requirement	A requirement that must be satisfied in order to reduce security risks to an acceptable level and/or to meet statutory, regulatory, policy, contractual and other security obligations.
Security Zone	An area to which access is limited to authorized, appropriately security screened personnel and to authorized escorted visitors.
Sensitive Information / Assets	Refers to information or assets that requires protection against unwarranted disclosure as compromise would reasonably be expected to cause injury in either the national or non-national interest. (i.e. Classified or Protected information and assets).
Unauthorized Access	Access to assets by an individual who does not have the proper security screening level and/or does not have a need to know.
Violation	An act or omission, deliberate or accidental that does not result in the actual or possible compromise of Classified or Protected information or assets

5. Security Roles and Responsibilities

The following section outlines the roles and responsibilities of security teams within GC departments and agencies, and reflects the requirements outlined in the DSM. While names or classifications for security team members may differ between GC departments and agencies, it is important to align these teams with the following descriptions to ensure clear roles and responsibilities are identified.

5.1. Chief Security Officer (CSO)

As per section 4.1.7. of the DSM, the CSO is responsible for: "Ensuring that any significant issues regarding policy compliance, suspected criminal activity, national security concerns or other security issues are assessed, investigated, documented, acted on and reported to the deputy head [of their department or agency] and, as required, to the appropriate law enforcement authority and/or security and intelligence agency (see Appendix I: Standard on Security Event Reporting), and to affected stakeholders, and as required, cooperating in any resulting criminal or other investigation(s)".

The CSO should support the security inspection process by providing security related leadership and guidance to all authorized individuals in order to properly define, document and implement security inspection protocols for all GC facilities. The CSO should also ensure the completion of a Threat and Risk Assessment (TRA) of the organization's facilities, at a minimum of every five years, or if there have been changes in the security environment or

threat landscape.

5.2. Building/Unit Security Coordinator

The Building or Unit Security Coordinator is responsible for ensuring that security inspections at GC facilities are conducted in accordance with the standards developed by their security units/sections. They may be responsible for forming teams of security inspectors to perform security inspections within their facilities, providing training to the inspection team members and ensuring that security incidents at GC facilities are reported in accordance with the organization's security policies and standards. When there is a change in the security environment, security coordinators may support departmental security units/sections in increasing the frequency of security inspections as well as administering other security measures to increase security readiness levels. The security coordinator can assist in the security inspection process by providing employees with advice and guidance on safeguarding protected or classified material.

5.3. Security Unit/Section

A GC departmental or agency security unit/section is responsible for the development and implementation of security inspection standards, and providing advice and guidance to security coordinators, the CSO and other stakeholders on security inspection matters (ie. policy requirements, security inspection strategy development, security incident reporting, etc.). As part of the administration of an organization's security program, Security Units/Sections should also develop tools and awareness training materials, provide advice related to the application and interpretation of security inspections, and address issues of non-compliance related to the application of departmental security standards.

Security Units/Sections should ensure that security inspections are carried out by an authorized security inspection team in accordance with this guide. They may advise security coordinators how to develop a security inspection team of their own, or create one within the Security Unit/Section to provide the service. The frequency of additional security inspections for their respective area should be based on the findings of the security inspection and recommendations derived from a TRA.

5.4. Security Inspectors & Security Inspection Teams

An authorized security inspector is a person delegated by an organization's departmental or building security section/unit to conduct a security inspection. A security inspector must possess a personnel security clearance or status that is commensurate with the highest category of information and assets being stored and processed within the area being inspected. An organization's departmental or building security team can nominate various security inspectors to form a security inspection team.

When forming a security inspection team, GC departments and agencies should ensure that inspection teams are composed of individuals who have a solid background and knowledge of the security inspection process and that all inspectors are provided with baseline training and awareness sessions on conducting security inspections. GC departments and agencies

should also consider the experience level of the inspectors and make every effort to comprise the team of a junior and senior member. This may encourage knowledge sharing and ensure best practices when conducting security inspections.

5.5. Directors

For the purpose of this guide, directors are responsible for ensuring all individuals within their area of responsibility have access only to the information and assets required for their position based on the need-to-know and need-to-access principle. Directors should also help ensure that all individuals are informed of the security inspection standard and that security inspections will be performed. Directors are responsible for ensuring that employees understand their obligation to safeguard information and assets.

Directors should work collaboratively with department or agency security personnel to ensure that any instances of non-compliance related to safeguarding sensitive information and assets are addressed and documented. Directors should ensure that individuals are provided the required security equipment to carry out their duties to ensure the security of sensitive information and assets (ie. abiding by a clean desk policy, and securing sensitive documents and IT peripherals at the end of each work day). They should also ensure that up to date physical security and security inspection training/awareness material is available.

5.6. Managers and Supervisors

As per section 4.4.2 of the DSM, supervisors are responsible for: "Ensuring that individuals are informed of their security responsibilities and that employees are provided with security awareness and training to maintain the required knowledge and skills to meet their responsibilities".

Managers and supervisors are responsible for working with departmental security teams/units to implement the findings and recommendations of security inspections as well as addressing issues or instances of non-compliance (ie. security violations) with individuals who have not adhered to the security measures.

5.7. Employees

As per section 4.5.1 of the DSM, employees are responsible for: "Adhering to government security policy and departmental security practices, including safeguarding information and assets under their control, whether working on-site or off-site".

Employees at all levels must assume responsibility and follow their department or agency's security policies and procedures for safeguarding sensitive information and assets in both physical and electronic form. It is important for employees to immediately report any security related incidents to their managers. An individual must immediately report the loss (whether accidental or suspicious) of protected or classified material to their manager or security office to help reduce the impact of a possible compromise.

6. Security Inspections

6.1. Legal and Privacy Considerations

When security inspections are conducted, it is important to note that the parameters of the inspection should follow GC collective agreements and staffing legislation. During the security inspection of an employee's assigned office or workstation, each employee's rights to privacy must be respected, and steps must be taken to respect applicable legislation and acts. These include, but are not limited to the Privacy Act, the Canadian Charter of Rights and Freedoms, and the Canadian Human Rights Act.

Although workspaces and furniture provided to employees belongs to the GC, during security inspections, the expectation of employee privacy remains in place. Employees may have personal belongings in their workspaces, and the Security Inspection Team should not search or open personal belongings or read or remove personal information found during the inspection. If during the course of the security inspection illegal items are found, the matter will be referred to the departmental security unit or police for investigation. Individuals may be subject to other forms of legitimate search and seizure under applicable criminal and civil laws as a result of a lawful security inspection.

Retention periods for inspection records should be determined and managed by the respective GC department or agency. Library and Archives Canada facilitates may assist departments and agencies with advice concerning specific retention periods.

6.2. Planning Security Inspections

When planning security inspections, security inspection teams should assess the risk environment of the areas being inspected. A TRA may need to be completed to help determine security inspection frequency at a facility. The SCOE Tool Kit also can be used for determining frequency of inspections. Security inspections should be conducted preferably outside of core working hours or while individuals or groups are away from the workplace. The Director and the security coordinator should be informed of the planned inspection in advance of the inspection date to ensure it is administratively feasible to conduct an inspection on the specified dates. In order to protect the integrity of the security inspection process, individuals working in the area should not be advised of the impending security inspection.

When forming teams for security inspections, departments and agencies should carefully consider the knowledge and experience level of the inspectors, how many inspectors are required based on the size and number of spaces to be inspected, and the categorization of material stored within the space. In order to maximize safety and ensure the integrity of the inspection process, security inspection teams should consist of at least two security inspectors.

Prior to conducting a security inspection, security inspectors should confirm that they have physical access and the appropriate security clearance for all physical security zones to be

inspected. When planning for inspection day, individual inspectors or inspection teams should ensure that they have the equipment needed to facilitate a proper inspection, including a notebook and pen or text recording device to document observations made during the inspection process, a device to take photographs (if appropriate to the physical security zone or operational situation) to visually document any findings, and an approved security container and lockable carrying case to secure material if any is found.

Please note that security inspectors and inspection teams must take care to not photograph protected and classified materials, locations, security controls or installed security devices and respect access restrictions for electronic devices in sensitive areas.

The Security Center of Excellence has produced a Security Inspection Risk Assessment Tool, available on GCcollab to assist security functional specialists to objectively and consistently determine the frequency of security inspections within a facility.

6.3. Conducting Security Inspections

Inspectors should follow specified guidelines for conducting security inspections and produce reports on the outcome of the inspection. This information is more fully defined in Annex B Section 2 and includes the following:

- A comprehensive visual inspection of employee workspaces. This should include offices and cubicles, desk surfaces, unlocked or open drawers or cabinets, mailboxes, waste and recycle bins as well as printer, scanner and shredder trays;
- Verification that electronic devices are properly secured (if applicable); and
- Validation that security containers or cabinets containing protected and classified material are properly secured.

When conducting an inspection, security inspectors should take their time and carefully search through all areas within the inspection zone. Employees may have personal belongings in their workspaces, and the Security Inspection Team must not search or open personal belongings, read or remove personal information or items found. If any personal items are found by security inspectors, it can be recorded in notes that these items were left untouched.

During the security inspection, the security inspector should ensure that unsecured items are secured in accordance with departmental policy and GCPSG-007 Transport, Transmittal and Storage of Classified and Protected Material Guide and locked in an approved security container or locked office. If unsecure protected or classified material is found during the security inspection, the security inspection team has the authority to remove the material in order to ensure it is properly secured.

If any material has been removed for safekeeping, the security team must store the item in the approved security container and physical security zone required for the categorization of material seized. The material should be accessible by the department or agency's security unit so that it may be returned to the owner as soon as possible. Any items that are removed from an office or workstation must be marked with the name of the employee, the office or

workstation number. If secure storage of the material is not possible and the owner is unknown or unavailable, the security inspector should secure the material to the best extent possible, advise senior management and arrange for the immediate handover to a person from the section responsible with the appropriate security clearance and need-to-know.

7. Outcomes

Once an office or workspace has been inspected, the security inspector or inspection team should leave a security inspection notice. This notice should inform the occupant(s) of the results of the inspection, any deviations from departmental security policies or standards that were found, items that were removed from the workspace and where they can be recovered. This notice should be left in plain view for the workspace being inspected so any occupants are aware an inspection has occurred.

Any observed deviations during an inspection should be labeled by the security inspector or inspection team as a security infraction. A breakdown of the security infraction levels, a general description of each infraction level, and recommended corrective administrative measures for each level are defined in Figure 2. Please note that these levels are not prescriptive and only serve as a general guideline; individual organizations should adapt these levels to their own security compliance standards and frameworks.

Security infractions are calculated based on violations within a security infraction category and not by the number of violations found within that category. For example, it would only be considered one infraction if a filing cabinet is left unlocked, even if there are several sensitive documents contained in the cabinet or if a file folder is left unsecured and contains several sensitive documents within the folder.

Security infractions are not meant to be punitive measures designed to force compliance with, nor punish offenders who are found to break departmental security policies. In most cases, security infractions should be considered a means to demonstrate and communicate to employees the importance of safeguarding GC information and assets. The table in Figure 2 offers some suggestions to address security infractions depending on their severity.

Upon completing a security inspection, the security inspector or inspection team should review the findings of the inspection, including any security infractions discovered, with the supervisor or manager of the inspected workspace as soon as possible. The findings of the inspection should also be reviewed with the employee to either provide recognition of a job well done or to provide them with information on what was found, and issue guidance on the proper security safeguards to help prevent reoccurrences or further non-compliance.

If a security inspection team discovers a severe security infraction or evidence of a possible breach or compromise (i.e. Infractions that look deliberate, repeated patterns, infractions involving information of a very high categorization level or serious criminal acts) they must take appropriate action to document the event, and begin an internal investigation liaising with relevant internal and external stakeholders as appropriate. Actions could be taken depending on

the nature or severity of the infraction as discussed in Figure 1.

Figure 1: Potential escalation of security infractions post-investigation

Infraction Category	***Potential Escalation***
Potential Disciplinary Action for Employee	• Departmental Labour Relations Team • Departmental Values and Ethics Team
Criminal Matters	• Law Enforcement Officials
Issues Regarding National Security Issues or Highly Classified Information	• Canadian Security Intelligence Service (CSIS) • Royal Canadian Mounted Police (RCMP)
Unauthorized Disclosure of Cabinet Confidences	• Privy Council Office (PCO)
Unauthorized Disclosure of Signals Intelligence (SIGINT)	• Communications Security Establishment (CSE) via Departmental Communication Intelligence Control Officer (COMCO)

Please note that departmental security teams should never unilaterally or independently consult with internal or external stakeholders on serious security infractions without first discussing or reporting the event to their respective CSO.

The findings of all security inspections should be compiled into a security inspection report which should be sent to the organization's security group. The report should contain a summary of workspaces inspected, the findings, and a summary of any security infractions identified. The report can also contain recommendations for senior management to review and determine what supplementary measures should be taken. A sample outline of a security inspection report can be found in Annex B.

Figure 2: Security infraction severity level

Severity Level	*Type of Security Infraction description*	*Corrective Administrative Security Measures*
1	First Notice of Security Infraction involving Protected A or B information and assets.	• A notification is sent to the individual and their direct supervisor.
2	Second Notice of Security Infraction involving Protected A or B information and assets. or First Notice of Security Infraction involving Confidential/Secret information and assets.	• A notification is sent to the individual, to their direct supervisor and to the next level of management. • The individual may be required to take or review a security awareness training (e.g., COR310 at the Canada School of Public Service or any other internal security training made available to them).
3	Third Notice of security Infraction involving Protected A and B information and assets. or Second Notice of Security Infraction involving Confidential/Secret information and assets.	• A notification is sent to the individual, to their direct supervisor and to the next level of management. • The individual may be required to attend a mandatory security briefing from the Departmental Security Unit/Section. • The individual may be required to attend a security interview with the Departmental Security Unit/Section to determine if a review of their security clearance and/or status is required. Based on the outcome of the interview, the case may be elevated to an Infraction Severity Level 4.
4	Over three Notices of Security Infraction involving Protected A and B information and assets. or Over two Notices of Security Infraction involving Confidential/Secret information and assets. or Any Notice of Security Infraction involving Protected C or Top-Secret information and assets	• A notification is sent to the individual, to their direct supervisor and to the next level of management. • The security screening review process may be initiated. • The individual may be required to attend a mandatory interview with the Departmental Security Unit/Section.

Notes:
1. A Notice of Security Infraction may pertain to electronic documents or systems.
2. Any Notice of Security Infraction considered criminal in nature may result in legal prosecution under the applicable laws subject to review and investigation by an organization's security unit.
3. Notice of Security Infraction severity are measured through levels 2 to 4 and may result in disciplinary actions. It is important to note that this is not part of the inspection process and corrective action should be determined by the GC department or agency. Decisions are made at the discretion of the CSO or Departmental Manager.
4. Should the individual's security clearance and/or status be revoked following a review process by their organization, the individual may no longer meet the conditions of employment. Human Resources or Labour Relations may need to be consulted

8. Monitoring and Reporting Requirements

Security inspection and infraction results can assist senior management within GC departments and agencies with making informed decisions and identifying mitigation measures to ensure the proper safeguarding of all protected and classified material. Security inspection reports should

be reviewed by departmental security sections/units on a regular basis, noting instances of repeated and severe security infractions. This will enable proper monitoring of the effectiveness of compliance and to identify any changes that might be required to manage and reduce security infractions.

One metric that GC departments and agencies may use is a security compliance rate. Outlined further in Annex C, a security compliance rate can be calculated by dividing the number of infractions by the number of employees and multiplying the value by 100 to get the percentage. This value, when compared with the GC department or agency's established risk tolerance, can assist departmental security teams in assessing levels of non-compliance and whether additional corrective measures should be put in place to mitigate the types and levels of infractions found during the inspection process. Some corrective measures may include additional or enhanced security awareness training or strengthening policies and procedures.

Statistical data on inspections and infractions should be maintained by departmental security sections/units for trend analysis. Reviewing this data can help determine if a GC department or agency's security posture is improving or deteriorating, and if systemic security issues are present which require more focused attention to address. As part of this review, consideration should be given to how to reduce recurrence of future infractions which can be done through a series of complimentary security measures. These can include, but are not limited to training and awareness sessions for employees on proper security protocols and procedures, technical barriers to prevent circumvention of security controls, and processes and procedures to monitor employee access to sensitive information.

The results of the analysis should be included in the departmental security plan, based on the identified trends and risks associated with employee non-compliance. This review should include a communication plan for employees as part of security education and awareness and ways to reduce further issues of non-compliance. Additional measures may be required and could include, enhanced physical security access control measures, IT controls, monitoring and increased security inspections.

These processes allow department security sections/units to monitor security compliance and advise their CSO on potential security risks and recommended administrative corrective measures. It can also serve as a foundation from which CSOs manage security infractions and enhance the security awareness culture in their organization.

9. Reference and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- GCPSG-015 – Guide to the Application of Physical Security Zones
- GCPSG-007 – Transport, Transmittal and Storage of Classified and Protected Material Guide
- GCPSG-001 – Equipment Selection Guide for Paper Shredders
- Security Centre of Excellence (SCoE) Security Inspection Risk Assessment Tool , available on

10. ANNEX A – Notice of Security Inspection

While this workspace was unattended, a Security Inspection Team conducted an inspection to determine if sensitive information and assets were protected in accordance with GC security policy and security practices.

Security Inspections are conducted in accordance with RCMP Guide GCPSG-005 Security Inspections Guide and departmental policy.

Date: _____
Time: _____
Office/Cubicle number: _____
Department: _____

Security Inspection Findings:
☐ This workstation complies with the organization's security policy and practices.

☐ Sensitive information found unsecured.
☐ Sensitive assets found unsecured.
☐ Computer left unsecured.
☐ Building Access Card/token/keys found.
☐ Personal electronic device found connected to computer equipment.
☐ Password or password-like combination found.
☐ Office door found unlocked (applicable to enclosed offices).
☐ Alarm not activated (may be applicable to enclosed offices).
☐ GC credit card or cash/cheques found.
☐ IT portable devices found.
☐ Cabinets or drawers appearing to contain protected or classified information or assets found
unlocked.

☐ Other_____
_____
_____

☐ Unsecure items were removed and placed in a secure container at the departmental security office.
Please contact _____ to recover the items.

11. ANNEX B -Security Inspection Report/Checklist

Security inspections are required to ensure protected and classified information and assets are safeguarded in accordance with the DSM. This example report should be left at the workstation or office by Security Inspection Teams after carrying out a security inspection. The Security Inspection Risk Assessment Tool is available on GCcollab to assist security functional specialists to objectively and consistently determine the frequency of security inspections within a facility.

Reminder:

- A Security Inspection Notice (Annex A) is to be left in plain view in every workstation that is inspected to inform the occupant that a Security Inspection took place and whether the office/workstation is properly secure.
- A Security Incident Report/Checklist (below) should be completed when documenting all security violations.
- An Outcome of Inspection(s) report should be submitted to the Program and Service Delivery Manager (Annex C).

Inspection Details

Date:	
Time:	
Department:	
Location:	
Name of Manager:	
Date of Last Security Inspection:	

Security Inspection Team		
1	**Name:**	
	Position Title:	
2	**Name:**	
	Position Title:	
3	**Name:**	
	Position Title:	
4	**Name:**	
	Position Title:	

Security Inspection Report

SECTION 1 – ADMINISTRATIVE SECURITY CONFIRMATION Note: The Security Inspection Team is to collaborate with the Program and Service Delivery Manager and/or the Building/Unit Security Coordinator to collect the necessary information for Section 1.			
#	**Inspection Criteria**	**Response:**	**Additional Comments**
1.	Is there a Building/Unit Security Coordinator identified for the area?	☐ Yes ☐ No	Name of Building/Unit Security Coordinator:
2.	a. Does a key ledger exist for the area? b. Are all keys identified in the key ledger accounted for? Note: A key ledger is used to track and document the number of mechanical keys and who they are issued to.	☐ Yes ☐ No ☐ Yes ☐ No	
3.	Has the access list recently been reviewed and updated accordingly?	☐ Yes ☐ No	
4.	Do all individuals working in the area possess the appropriate personnel security screening status/clearance?	☐ Yes ☐ No	
5.	Access into a Security and High Security Zone (See note in #7) must be continuously monitored. Is the alarm being properly set when the space is unoccupied?	☐ Yes ☐ No	
6.	Is there an access logbook for individuals to sign in and out? *Note: A High Security Zone is an area to which details of access are recorded and audited. In some cases, card in/out card readers are used to capture this information.	☐ Yes ☐ No	
7.	a. Are there documented response procedures in place in the event of an alarm? b. Are the response procedures updated appropriately (i.e. are proper contacts identified)?	☐ Yes ☐ No ☐ Yes ☐ No	

SECTION 2 – SECURITY ZONE INSPECTION			
#	**Inspection Criteria**	**Response**	**Additional Comments**
1	Sensitive information must be destroyed in accordance with the Secure Destruction Standard a. Is there a shredder in the area? b. Is there a label affixed to the shredder to identify the classification level of information the shredder is approved to destroy?	☐ Yes ☐ No ☐ Yes ☐ No	
2	Is sensitive information being thrown away in the garbage can or recycling bin? Note: If sensitive information is found in the garbage can or recycling bin during the inspection, the Security Inspection Team must claim the information and ensure it is properly secured and destroyed.	☐ Yes ☐ No	
3	Can sensitive information be viewed through any window?	☐ Yes ☐ No	
4	Are personal electronic devices (i.e. personal cell phone, USB key, etc.) connected to GC computing equipment? Note: If personal electronic devices are found to be connected to computing equipment during the inspection, the Security Inspection Team must disconnect these devices.	☐ Yes ☐ No	
5	Is protected and/or classified information and assets (i.e. portable storage media) secured in accordance with GCPSG-007 Transport, Transmittal and Storage of Protected and Classified Material? Note: To determine if protected or classified information is in a pile of papers on a desktop or other furniture, visually inspect the papers for any sensitive information or marked headers.	☐ Yes ☐ No	
6	Are all security containers (including safes, filing cabinets, desk drawers, etc.), appearing to contain protected or classified information or assets locked? Note: • To determine if a security container is unlocked, pull on a drawer or door to see if it opens. • If the security container is unlocked, complete a visual inspection to determine if it appears to contain protected or classified information or assets.	☐ Yes ☐ No	
7	Are all keys removed from their cabinets and not stored visibly on the desktop?	☐ Yes ☐ No	

	Note: If unsecure keys are found during the security inspection, the Security Inspection Team are to remove and secure keys.		
8	Are any keys easily found around or in office furniture? Note: • To determine if a key can be easily found, open unlocked drawers to visually see a key, check under overhead bins, check in cubicle wall flaps and other common hiding spots to identify if a key is present. • If a key is found, test it on the cabinets at the employees' office or workstation and complete a visual inspection of the inside of the cabinet to determine if it appears to contain protected or classified information or assets.	☐ Yes ☐ No	
9	Are passwords or password-like combinations documented and exposed? Note: • To search for a password or password-like combination that is not readily visible on the desktop, lift common items such as the phone, keyboard and desktop calendars for a visual inspection. • If passwords or password-like combinations are found during the security inspection, the Security Inspection Team must ensure they are removed.	☐ Yes ☐ No	
10	Are rooms that are supposed to be secured properly locked and alarmed? If a room is found to be unsecured, proceed with inspecting the office as described above.	☐ Yes ☐ No	

12. ANNEX C – Security Compliance Rate

The compliance rate is determined by the organization's total infraction percentage and is calculated by the of the total number of security infractions and is divided by the number of employees, multiplied by 100%. The organization's risk framework should be used to assist in determining acceptable level of non-compliance.

**Calculated as:* $100\% - \left(\#\frac{infractions}{employees} \times 100\right)$

Below is a summary of the security inspection that was conducted within your area of responsibility:

Number of Employees	Number of Notices of Infractions	Compliance Rate*

Type of Infraction	Number of Infractions
Protected A and/or B information	
Protected C information	
Classified Information below TOP SECRET	
TOP SECRET Information or above	
Computer unsecured	
Building Access Card/token/keys	
Personal electronic device found connected to computer equipment	
Password or password-like combination found	
Office door found unlocked (applicable to enclosed offices)	
Alarm not activated (may be applicable to enclosed offices)	
GC credit card or cash/cheques found	
IT Portable devices	
Cabinets or drawers appearing to contain protected or classified information or assets found unlocked	
TOTAL	

Security Violation Summary		
#	**Description of the Security Violation**	**Security Incident Report #**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
Total Number of Security Violations Identified during Security Inspection:		

NOTE: A copy of this Security Inspection Report is to be sent to the Manager and Departmental Security/Unit Section.

13. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-005 (2023) - Security Inspections Guide, for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2023.08.09 12:56:19 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve GCPSG-005 (2023) - Security Inspections Guide, for approval.

Lafrance,Gaetan Joseph,000133993

Digitally signed by Lafrance,Gaetan Joseph,000133993
Date: 2023.08.09 13:36:05 -04'00'

Gaétan Lafrance
Acting Director, Physical Security
Royal Canadian Mounted Police

Date