Physical Security Considerations for Remote and Telework Environments

GCPSG-008 (2022)

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

Publication Issued: 2022-XX-XX
Updated:

Foreword

The Remote/Telework 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 security considerations in a Remote/Telework location for departments, agencies and employees of the Government of Canada.

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

Effective Date

The effective date of GCPSG-008 (2022) Physical Security Considerations for Remote and Telework Environments is 2022-XX-XX.

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 guide is to provide Government of Canada (GC) employees with information on assessing physical security and applying the appropriate protection and storage requirements for GC information and assets while working in a location other than the designated worksite. Employees should also consult their departmental security policies, directives, standards, processes, and guides for additional information and direction.

This guide addresses the increased threats posed by physical access to information and devices while in a Remote/Telework environment and provide GC employees tools to protect themselves, information, assets or devices in a Remote/Telework setting.

1.2. Applicability

This guide identifies physical security requirements for Remote/Telework locations including the handling of sensitive hard copy documents, information and assets. This guide addresses the physical security of electronic devices but does not address the IM/IT security (cybersecurity) for GC systems used in the creation, processing, or storage of electronic information.

Some GC departments and employees may choose a hybrid work agreement rather than a full time Remote/Telework agreement. A hybrid work agreement is defined as an employee working part-time at a GC designated work location and part-time at a Remote/Telework location. This guide is specific to the Remote/Telework location and does not detail the security requirements for a GC designated worksite. Choosing a hybrid work agreement rather than a full time Remote/Telework agreement does not allow for security control requirements to be relaxed or omitted at the Remote/Telework location. All recommendations in this guide should still be followed.

This guide should be used to support decision making for Remote/Telework requests however, should not be considered the sole source for physical security concerns for Remote/Telework. Other RCMP LSA guides may be required to fully assess Remote/Telework security and are available at Lead Security Agency for Physical Security - Royal Canadian Mounted Police (rcmp-grc.gc.ca).

1.3. Information Technology Considerations

With the constantly evolving threat landscape, and the convergence of physical and information technology (IT) security, the requirement to assess the risk of any application and/or software connected to a network to operate and support equipment in 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

Abbreviation / Acronym	Meaning
CHRO	Chief Human Relations Officer
CIO	Chief Information Officer
CSE	Communications Security Establishment
CSO	Chief Security Officer
CCTV/CCVE	Closed Circuit Television / Closed Circuit Video Equipment
DND (NSC)	Department of National Defence (National Special Center)
GAC	Global Affairs Canada
GC	Government of Canada
IM/IT	Information Management and Information Technology
RCMP LSA	RCMP Lead Security Agency for Physical Security
SSC	Shared Services Canada
TBS	Treasury Board Secretariat of Canada
VPN	Virtual Private Network

4. Glossary

Term	Definition
Remote/Telework	This guide uses the generic term Remote/Telework to identify any combination of either remote or telework work performed in a location "other than the designated worksite".
Remote work	A term used to describe work being accomplished in a location that is not a designated worksite. This is an employer-driven process where the health and safety of its employees are of concern. These situations generally occur during temporary unforeseeable circumstances, such as pandemics, states of emergencies, inclement weather, etc.

Telework	Work performed by an employee from an alternate location other than a Government of Canada designated worksite, based on a voluntary request from an employee, subject to operational requirements and management approval.
Hybrid Work	A combination of Remote/Telework and work from a designated GC workplace.
Processing	The access, creation, development, update, amendment to, or working with GC information.

5. Context

This guide will refer to remote work or telework as Remote/Telework and makes no distinction between the two when it comes to the physical security assessment and physical security control requirements. Additionally, a hybrid working arrangement, part time Remote/Telework and part time work in a designated GC work location or GC co-working site, does not reduce or change the physical security requirements at the Remote/Telework location.

Historically, remote working situations have been in response to an unforeseen circumstance whereas telework is a response to a request from an employee. Remote/Telework has become increasingly popular across government departments as trust in systems, processes and employees build. Treasury Board of Canada Secretariat (TBS) defines Remote/Telework as either Remote Work or Telework:

5.1. Related Security Policies

Overarching TBS Policies and specific departmental standards bind employees who are in Remote/Telework locations even though they are working outside the bounds of a traditional physical workspace. Remote/Telework allows for the continuation of business operations while an employee is physically located away from government owned and operated facilities. Although not an exhaustive list, the following TBS Security policy instruments apply when considering Remote/Telework:

- Policy on Government Security, July 1, 2019;
- Directive on Security Management, July 1, 2019; and
- TBS, "Directive on Telework, TBS, April 2020; and
- TBS, "Guidance on optimizing a hybrid workforce: Spotlight on Telework". (available from TBS)

5.2. Increased Threats

Remote/Telework can increase the likelihood of compromise of an organization's sensitive information. Information processed in a Remote/Telework setting may be exposed to unauthorized individuals such as family, friends and others. This may prompt threat actors, whether organized or opportunistic, to target information through different methods, which may include:

- Physical access to information and devices;
- Theft of information or devices;
- Eavesdropping during meetings and telephone conversations; and
- Overviewing of information or devices.

6. Remote/Telework Decisions

In the modern workplace, allowing workers to Remote/Telework is becoming the norm. Issues related to improved health, inclusivity and pollution are drivers promoting Remote/Telework[1]. In many instances GC employees work with sensitive information which, when processed in a Remote/Telework location presents challenges for physical security. In order to reduce security vulnerabilities posed by Remote/Telework, the RCMP LSA recommends the following as a part of departmental risk management.

- Chief Security Officers (CSOs) should be involved in supporting managers within departments so that informed risk-based decisions related to Remote/Telework can be made;
- CSOs, managers, supervisors and employees should make every effort to promote and recommend that Remote/Telework options prevent or limit the use of hard copy material as much as practicable; and
- CSOs and managers along with departmental HR groups have the authority to identify if an employee's position can be designated to undertake Remote/Telework; employees should not be permitted to make decisions on this unilaterally as some positions may not be conducive to Remote/Telework due to the job requirements or other security concerns.

6.1. Remote/Telework Limitations

In accordance with TBS policies, all individuals having access to protected and classified information must have the appropriate security status or clearance and the need-to-know. It is recommended that Protected C, Secret and Top Secret information only be processed in the appropriate zone in a designated GC worksite. Processing Protected C, Secret and Top Secret material in a Remote/Telework location should be avoided (it should be noted here that TS SCI info CANNOT be processed in a Remote/Telework environment. CSE and the DND National Special Center are the only authorities that accredit locations to process, store and discuss this information at this categorization level). This is particularly relevant for hard copy information where the necessary storage requirements may not be achievable. CSOs or higher level management up to the Deputy Head are responsible to risk manage authorizations for employees to process and store all categorizations of hardcopy information at the Remote/Telework location.

6.1.1. Protected A and B

This material may be processed and stored at Remote/Telework locations outside a designated GC workplace when physical protections recommended within this guide are employed.

[1] TBS Directive on Telework

6.1.2. Confidential and Secret

RCMP LSA recommends all Remote/Telework requests where Secret material may or will be processed are closely monitored. Processing hardcopy material of this categorization in Remote/Telework location is not recommended and should be avoided wherever possible. Any handling of Confidential or Secret material while en route to, or processing in location at the Remote/Telework location should be considered a higher risk. CSOs are responsible to risk manage these decisions and should verify each request in this category individually, ensuring that all required security controls are in place.

6.1.3. Protected C and Top Secret

Handling of Protected C and Top Secret material while en route to, or processing at the Remote/Telework location should be considered an unacceptably high risk. CSOs are responsible to risk manage these decisions and should verify each request in this category individually while considering all possible options to avoid Remote/Telework. If unavoidable, CSOs should ensure that all required security controls needed for a High Security zone are in place including a complete Threat and Risk Assessment (TRA). RCMP LSA does not recommend Remote/Telework be approved where Protected C and Top Secret material will be processed.

6.2. Management Responsibilities

Departments must assess all Remote/Telework situations and risk manage work solutions while considering TBS policies, RCMP LSA Guidance documents, and organizational directives and procedures. Approval may be granted individually, to a group, department, or agency by the CSO or delegate based on each organization's risk management process and tolerance. In some cases, this may be at the Deputy Head or higher level of management. Consideration should be given to the location of the requested Remote/Telework Environment. It should not be located in a high crime or dangerous area of the city.

Managers should advise employees that they are responsible for and must take reasonable care to protect sensitive government information and assets against unauthorized disclosure, loss, theft, fire, destruction, damage, or modification. Managers should remind employees to follow GC, departmental and security policies governing the use of electronic devices.

It is recommended that paperless systems be used whenever possible and (if applicable) any original files remain in the workplace. When paper documents are required, it is recommended that copies may be created for transport to the Remote/Telework location while all originals remain in the designated GC worksite. It is recommended to complete a tracking sheet for all Secret, Top Secret and Protected C paper documents taken out of the designated GC worksite in order to account for all files and to maintain file integrity. Managers and employees should sign out and in, all files removed and record the subject and number of pages in each file.

Remote/Telework agreements should be reviewed at a minimum annually to ensure there have been no changes to the Remote/Telework situation or location. Departments should also maintain tracking data for all employees on Remote/Telework agreements which should include:

- Names;
- Locations;
- Issued departmental equipment and assets; and
- Registries of information taken to the Remote/Telework location as deemed appropriate.

6.3. Employee Responsibilities

Employees at Remote/Telework locations must follow all security control requirements for the possession, handling, processing, storage, transportation, destruction and care of GC information and assets, and only use approved electronic devices for this purpose.

Employees should clearly understand and implement all Remote/Telework security control measures that contribute to the secure processing of GC information at their location. Employees should:

- Follow all policies and procedures that outline the acceptable use of corporate devices and the management of corporate information which may include Managing government information when working remotely - Canada.ca;
- Follow all departmental and GC security policies, for the protection of information and assets such as:
    - Transportation, storage and destruction of information and other assets;
    - Guarding against unauthorized disclosure of information during processing or, discussions;
    - Avoid discussing protected or classified information on unapproved devices, while on speaker-phone, or with cohabitants.
    - Using all equipment provided such as headsets, secure containers;
    - Set up their workspace away from windows and in such a manner that prevents unauthorized viewing of computer monitors;
    - Disconnect any virtual assistance devices such as Google Home, Alexa, etc. to prevent those services from recording work related conversations; and
    - Reporting any security incidents such as loss of information, or theft of electronic devices.
- Ensure they know who to contact in the event of any issues that may affect the security of sensitive material, especially if they experience security issues, or if devices or information are lost or stolen;
- Complete all required training on security issues and best practices, such as being aware of surroundings, information protection and storage;
- Follow departmental process for the storage of information in corporate repositories;
- Follow requirements and procedures for electronically securing devices, such as enabling multi-factor authentication;
- Follow best practices for physically securing devices, such as never leaving devices unattended in public; and
- Understand their responsibilities for maintaining the status/usability of their Remote/Telework location (utilities, high-speed internet service, and insurance).

6.4. Security Equipment

Each department should develop procedures to support and promote the use of security equipment and approved electronic devices at a Remote/Telework location in accordance with the categorization of material. The use of such equipment should support the employees need to safeguard information and assets during transport, while in the Remote/Telework environment and promote the security of information and electronic devices. Equipment items could include; secure carry bags, storage cabinets, headsets, computer privacy screens etc., Employees should be provided equipment which supports and promotes secure processing, storage, and transport of GC information.

Departments should establish processes and systems that employees can use to access procurement options, supply and delivery of suitable processing and security equipment.

6.5. Remote/Telework Abroad

The RCMP LSA does not recommend approving requests to Remote/Telework from international locations and determining whether (or not) to approve these requests is a very complex issue. Refer to section 8 of this guide for information on international Remote/Telework requests.

7. Storage Requirements – General

Every effort should be made to limit the need to process or store hard copy documents of any categorization in locations outside a GC controlled facility. Departments should supply and promote the use of secure electronic technologies to improve workspace functionality and decrease reliance on hard copy information.

All Information and assets whether in the Remote/Telework environment or a GC facility should be physically stored in accordance with RCMP LSA guidance and departmentally established security practices. When material is not in use, or when the employee leaves the Remote/Telework location, the employee should:

- Do a quick scan to ensure windows and doors are closed and locked;
- Make sure all documents are stored in accordance with RCMP LSA guides and departmental procedures and policies;
- Disconnect electronic devices from networks, systems, VPN's and power down the equipment;
- In accordance with the categorization of the information or assets, using the appropriate security container, lock up and separately secure electronic equipment, PKI cards/tokens, or other devices when absent from the Remote/Telework location;
- Close blinds or shades in the work area (if applicable);
- Arm alarm systems (if applicable); and
- If away from the Remote/Telework site for extended periods of time (i.e., vacation) consideration should be made to return and store information and assets at the designated

GC worksite. At minimum managers should be made aware of the storage arrangements in the Remote/Telework location.

7.1. Storage Requirements – Protected A, B,

Storage

Protected A, B information should be stored in a lockable container. At a minimum, Protected B and below information at the Remote/Telework location should be stored out of sight, and inaccessible to any unauthorized access when not in use.

Rooms/Offices

Access control measures including locked doors should be considered to limit unauthorized viewing or access.

7.2. Storage Requirements – Confidential and Secret

The RCMP does not recommend Remote/Telework on Confidential and Secret information or assets. When work on this level of information or assets cannot be avoided, the following guidance should be followed:

Storage

All information and assets marked Confidential or Secret should be stored in approved storage containers per the RCMP G1-001 - Security Equipment Guide. Approved security containers containing Secret information should be fastened to the building structure to prevent removal.

Rooms/Offices

A dedicated lockable room should be used for the processing and storage of Confidential or Secret material to limit unauthorized overview and access. The room should be locked using commercial grade hardware when not occupied. High value assets or monetary instruments should not be stored in the same container as other information or assets.

Monitoring

The RCMP LSA recommends that a monitored residential alarm system capable of initiating a response element be installed at Remote/Telework locations where Confidential or Secret material are processed or stored. Alarm systems should have as a minimum, window and door contacts, and motion detection capability in the room where the information is stored.

7.3. Storage Requirements - Protected C, Top Secret

The processing and storage of Protected C or Top Secret information outside approved GC facilities is considered an extremely high risk and is not recommended by the RCMP LSA. If unavoidable, a full site security assessment should be undertaken by departmental physical security, which would include a complete Threat and Risk Assessment. All security controls required for High Secure Zones in GC facilities should be used as a minimum standard for location fit-up.

8. International Remote/Telework

Many departments in the GC have employees assigned to work in locations abroad as part of their regular operational duties. This guide is not meant to affect already assigned positions such as those attached to Canadian Embassies and High Commissions. Global Affairs Canada (GAC) has an LSA responsibility for providing leadership, advice, and guidance regarding security at missions abroad and may be a good source of information should departments decide to approve international Remote/Telework requests.

The RCMP LSA does not recommend allowing Remote/Telework from international locations. Departments should be aware that any requests for international Remote/Telework requires a very intensive security assessment and approval process as well as an administrative and immigration assessment to ensure any requirements are uncovered. Departments who may allow international Remote/Telework should develop a process with considerations given for all security controls, risk assessments, approvals and briefings.

8.1. TBS Guidance

As per TBS - Guidance on optimizing a hybrid workforce, international Remote/Telework should not be the norm. Employees are expected to work from within Canada, except where normal duties require them to work abroad. Requests to work outside of Canada should be granted only in exceptional circumstances and be reviewed by the CSO, security functional specialists, the organization's Head of Human Resources and human resources specialists, and will require departmental approvals at management levels higher than the normal process for domestic telework; up to the Deputy Head. Risks associated with working outside of Canada carry serious implications not related to security such as, work visa and tax requirements, health care access and health benefits, public health and emergency response, and diplomatic relations. The ability for departments to provide adequate duty of care for employees may be limited in international locations. Requests for international Remote/Telework should:

- Only be considered under exceptional circumstances;
- Be limited to a specific defined period of time;
- Be subject to increased administrative scrutiny;
- Require a complete Threat and Risk Assessment (TRA) for the employee, country, and city of work; and
- Require additional or special approval from:
    - Deputy Head;
    - Department CSO;
    - Department CHRO;
    - Department CIO; and
    - Shared Services Canada (require SSC permission to use any GC device connected to an international internet network which connect to GC networks).

8.2. Personal Security (International)

In addition to the implications listed above, international Remote/Telework carries increased security risks for the individual and the GC. The Vienna Convention on Diplomatic Relations

(1963) would not apply to those GC employees working internationally who are not diplomatic staff or dependents. These employees will be subject to all local and state laws and not afforded diplomatic protections for information, assets or property, including GC information and assets. In some countries, this could create problems for the GC employee working on behalf of a foreign government in the Host nation territory.

Duty of Care responsibilities for employers may be limited internationally in cases of extreme weather, armed uprisings, or other such issues. Departments should be aware of the potential for these types of issues for employees working abroad prior to approving any international requests. Employees requesting to Remote/Telework internationally should also be made aware of these limitations.

The basic concepts of personal security that all Canadians take for granted may not exist in the international location. High crime rates, limited access to police or security services and sophisticated intelligence gathering services is a reality in many countries making the safety and security of the employee, their families and residences a concern. All evidence must be weighed against the benefits prior to approving any international Remote/Telework requests.

8.3. Physical Security (International)

In addition to the implications listed above, international Remote/Telework carries increased physical security risks. Employees working in international locations without diplomatic protections are subject to all local and state laws and the overall security situation of the country where they choose to work. Crime (including personal, property and intellectual crimes), limited policing, poverty, natural disasters, state sponsored activities, and xenophobic tendencies may all form parts of the overall security situation for the international location. Physical security controls for some international locations may be cost prohibitive or difficult to maintain without a departmental security presence. GAC, in their Lead Security Agency role, may be able to assist with the provision of advice on which security control measures may be required to protect GC personnel, information and assets.

The scope and conduct of an international security survey or TRA is beyond the parameters of this guide and it requires mentioning again that the RCMP LSA does not recommend approving international Remote/Telework requests. Prior to approving requests for international Remote/Telework, the ability of the department to implement and maintain the required security controls and measures should be considered.

The following is a list of security control measures that may be necessary to protect GC personnel, information and assets depending upon the specific security situation in the international location. This list is not exhaustive, as the requirements are highly location specific:

- Location, Location, Location – ensure the Remote/Telework environment is not located in a high crime or dangerous area of the city/country;
- Installation of security fences, walls or barriers surrounding the location including an anti-climb topper;
- Installation of CCTV/CCVE systems with recording and playback capability;

- Installation of residential security alarm systems with reliable response capability;
- The hiring of residential security guards;
- Installation of robust security locking hardware on all windows, doors, gates, etc.;
- The use of window film, bars or grills;
- Installation of door security gates, grills or trelly doors;
- The availability of safe havens or residential panic rooms;
- The availability and use of approved physical security containers for information and assets;
- The abilities of local emergency responders (police, fire, ambulance, etc.) and their contact details;
- Ensure there is adequate and available Embassy or High Commission of Canada Consular support mechanisms;
- Appropriate IT security measures (as required by SSC/CSE) are in place;
- Appropriate evacuation plans and safe third country contacts are available and contact information is available; and
- Ensure staff teleworking internationally receive country specific security briefings and training.

9. Other Security Considerations

9.1. Completing Security Awareness Training

As a condition for approving Remote/Telework applications, it is recommended that departments develop and deliver security awareness training to each employee either individually or in a group setting. Periodic security briefings and refresher training may also be considered.

9.2. Cohabitation

A valid security clearance is required for all employees and in exceptional circumstances, may be considered for cohabitants. This would be at the discretion of the CSO or higher level management when employees are required to Remote/Telework on Secret or higher information. Employees should report changes in cohabitation or any other factor that may call into question the security posture of the Remote/Telework location or the employees' security clearance/status.

9.3. Security Clearance/Status Expiry

Managers should routinely verify the employees' security clearance/status and highlight those that will expire during the Remote/Telework work period.

9.4. Transportation

Information and assets should be transported as per GCPSG-007 Transport, Transmittal and Storage Guide for Protected and Classified Information and associated departmental procedures when sensitive material is in transit. Employees should not make unnecessary stops when transporting information or assets; and at no time should sensitive information or assets be left unattended.

9.5. Control of Information and Assets During Processing

Employees should observe fundamental procedures to protect sensitive information when working in the Remote/Telework location. Employees should always conduct work within a dedicated space which can be secured from oversight by cohabitants or through windows and make every effort to ensure that conversations cannot be overheard.

Employees must avoid discussing protected or classified information on unapproved devices, while on speaker-phone, or with cohabitants. Information and electronic devices should be secured when unattended, using the computer lock screen and ensuring all paper files are secured within a suitable container.

9.6. Protection and Use of Electronic Storage Media

GC and departmental IT requirements do not allow for personal USB or other electronic mass storage devices to be used for the storage of protected or classified GC information nor that they be connected to GC computers or networks. Information and files may be stored on government issued approved encrypted devices that have been evaluated and approved by the departmental IT Security section. When not in use, approved USB and mass storage devices should be stored in containers appropriate to their security categorization level. Departments and agencies should establish clear employee guidelines on the appropriate use of USB devices.

9.7. Printing, Copying and Scanning

Connecting personal peripheral devices such as printers or scanners to GC workstations is not permissible. Under exceptional business circumstances, employees may request multifunction devices be used at the Remote/Telework location. Print using departmentally supplied devices; scanning or copying of GC information is not recommended. All departmentally supplied printers should be returned to the issuing department when no longer required. Requests for print capability should be initiated by the employee's manager and be reviewed and approved by both the CSO and departmental IT Security program.

9.8. Information and Asset Disposal

Protected and classified information and assets awaiting destruction should be treated in the same manner as all other information or assets. It may be stored securely at the Remote/Telework location while awaiting return to the GC worksite for destruction/shredding. Transport material for disposal in accordance with GCPSG-007 Transport, Transmittal and Storage Guide for Protected and Classified Information.

9.9. Returning Assets

Government supplied IT media and equipment should be stored securely at the Remote/Telework location until returned to the workplace following Remote/Telework use. Transport material in accordance with GCPSG-007 Transport, Transmittal and Storage Guide for Protected and Classified Information.

9.10. Checklists, Guides and Process Maps

Departments should develop checklists or process maps for managers and employees to follow to ensure that appropriate security controls and other measures are being used to mitigate risk. Tailor checklists to suit departmental requirements and include elements such as but not limited to ensuring:

- Employees have appropriate security clearance/status, and have a need to know;
- Employees have completed security awareness training;
- Employees are briefed on proper procedures to protect information at a Remote/Telework location; and
- Appropriate security controls are available and in place;

Security Centre of Excellences' tool for decision making on Remote/Telework is a good start for departments to review as they develop their own process for dealing with Remote/Telework requests. It is available at SCoEs' GC page, you need to have a GCCollab account and be a member of the group to view and use the toolkit.

Simple and effective Remote/Telework guides should be developed by each department or agency as quick reference on security "do's and don'ts" and to remind employees of their responsibilities when approved to work in a Remote/Telework location.

10. References and Related Documents

- CSE, CCCS, "Security Tips for Organizations with Remote Workers", ITSAP.10.016, May 2020
- CRA, "Managing Paper Documents in the Home Workspace", 2020
- Managing government information when working remotely - Canada.ca;
- TBS, "Directive on Telework, TBS, April 2020
- GC, "Coronavirus disease (COVID-19): Working remotely", January 2021
- Policy on Government Security, July 1, 2019
- Directive on Security Management, July 1, 2019
- Directive on Security Management - Appendix J: Standard on Security Categorization, July 1, 2019
- Directive on Security Management - Appendix B: Mandatory Procedures for Information Technology Security Control
- GCPSG-007 Transport, Transmittal and Storage Guide for Protected and Classified Information (Currently G1-009)
- RCMP G1-001 - Security Equipment Guide
- TBS, "Guidance on optimizing a hybrid workforce: Spotlight on Telework"

Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-008 (2022) – Physical Security Considerations for Remote and Telework Environments, for approval.

Nattress,Shawn Thomas,000302786 Digitally signed by Nattress,Shawn Thomas,000302786 Date: 2022.05.10 13:55:12 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve GCPSG-008 (2022) – Physical Security Considerations for Remote and Telework Environments.

St-Pierre,Andre Vincent,000171484 Digitally signed by St-Pierre,Andre Vincent,000171484 Date: 2022.05.11 14:29:39 -04'00'

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

Date