# Security Guide for SRCLs

V Division Fire and Safety Equipment Inspections
SRCL #: 2023-11118

Prepared by:
NWR Departmental Security Section
Royal Canadian Mounted Police

DSS Physical Signature: Godfrey,Tracy May,000161061

Digitally signed by Godfrey,Tracy May,000161061
Date: 2023.01.16 09:57:34 -06'00'

## General Security Requirements

**Description of Work:** "V" Division
Blanket SRCL for RCMP occupied buildings in V Division for building inspections, testing, repair and replacement of fire and safety equipment, including alarm systems and related materials (eg. lighting, strobes, etc.). All contractors will be escorted.

**Security Clearance:** RCMP Facility Access Level 2 (FA2) with Escort
*****NWR DSS Internal Use ONLY*** Intake Diary Date for SRCL (Expiry):** 2026-01-13

---

All contractors employed on this contract must support the RCMP's security environment by complying with the directives described in this document.

1. All Protected information (hard copy documentation) or other sensitive assets for which the RCMP is responsible will be shared with the contractor through pre-approved processes.

2. The information disclosed by the RCMP will be administered, maintained, and disposed of in accordance with the Contract. At minimum the contractor must follow the Policy on Government Security.

3. The contractor will promptly notify the RCMP of any unauthorized use or disclosure of the information exchanged under this contract and will furnish the RCMP with details of the unauthorized use or disclosure. (i.e. loss of sensitive information, accidental or deliberate.)

4. Photography is not permitted. If photos are required, please contact the Organization Project Authority and Departmental Security Section.

5. The use of personal property, e.g. desktop peripherals, communication devices, portable storage media such as USB sticks, in conjunction with RCMP technology is prohibited

6. The contractor is not permitted to disclose sensitive information provided by the RCMP, to any sub-contractors, without those individuals having the proper RCMP security level required to access the protected information.

7. The RCMP's Departmental Security Section (DSS) reserves the right to:
    - conduct inspections of the contractor's site/premises. Inspections may be performed prior to sensitive information being shared and/or as required (i.e. if the contractor's work location relocates). The intent of the inspection is to ensure the quality of security safeguards.
    - request photographic verification of the security safeguards. Photographs may be requested prior to sensitive information being shared and/or as required (i.e. if the contractor's work location relocates). The intent of the photographs is to ensure the quality of security safeguards.

- provide guidance on mandatory safeguards (safeguards as specified in this document and possibly additional site specific safeguards).

8. To ensure Canada's sovereign control over its data, all sensitive or protected data under government control will be stored on servers that reside in Canada. Data in transit will be appropriately encrypted.

## Physical Security

**1. Storage**: Protected information/assets must be stored in a container acceptable to the RCMP DSS. The container must be located (at minimum) within an "Operations Zone". As such, the contractor's facility must have an area/room that meets the following criteria:

| Operations Zone | |
|---|---|
| Definition | An area where access is limited to personnel who work there and to properly escorted visitors.<br><br>Note: The personnel working within the Operational Zone must:<br>• possess a valid RCMP Reliability Status (RRS), or<br>• be escorted by an individual who possesses a valid RRS |
| Perimeter | Must be indicated by a recognizable perimeter or a secure perimeter depending on project needs. For example, the controls may be a locked office or suite. |
| Monitoring | Monitored periodically by authorized employees. For example, users of the space working at the location are able to observe if there has been a breach of security. |

Note: Refer to Appendix A for more information on the Security Zone concept.

2. **Discussions**: Where sensitive conversations are anticipated, Operations Zones must have a stand off from public spaces or be designed with acoustic speech privacy properties (where the user has a reasonable expectation that they will not be overheard). For example, private room/office and/or boardroom.

3. **Production**: The production (generation and/or modification) of Protected information or assets must occur in an area that meets the criteria of an Operations Zone.

4. **Destruction**: All drafts or misprints (damaged copies and/or left over copies) must be destroyed by the contractor. Protected information must be destroyed in accordance with the RCMP's Security Manual. The equipment/system (i.e. shredder) used to destroy sensitive material is rated according to the degree of destruction. RCMP approved destruction equipment must be utilized.

   Approved levels of destruction for Protected B include:

   - Residue size must be less than 1 x 14.3 mm (particle cut).

   Note:

- If the contractor is unable to meet the RCMP's destruction requirements, all sensitive information/assets are to be returned to the RCMP for proper destruction.
- Any sensitive drafts/misprints awaiting disposal must be protected in the agreed upon manner until destroyed.

5. **Transport/Transmittal:** The physical exchange of sensitive information must follow the Contract. When a delivery service is used, it must offer proof of mailing, a record while in transit and of delivery.

| | |
|---|---|
| Transport | Transport: to transfer sensitive information and assets from one person or place to another by someone with a need to know the information or need to access the asset. |
| Transmittal | Transmit: to transfer sensitive information and assets from one person or place to another by someone without a need to know the information or need to access the asset. |

Note:

- For Transport of Protected "B" information (travel to/from neutral locations for meetings and/or interviews): In place of a single envelope, a briefcase or other container of equal or greater strength may be used. Double envelope/wrap to protect fragile contents or to keep bulky, heavy or large parcels intact.
- For Transmittal of Protected "B" information (Canada Post or registered courier): Address in a nonspecific manner. Add "To Be Opened Only By" because of the need-to-know or need-to-access principles when warranted.

## IT Security

### Appropriate Control of Protected A and B Information

#### Transport/Transmittal

1. If there is a requirement to send RCMP Protected A or Protected B information electronically, it must be sent using a FIPS 140-2 compliant portable storage device provided by the RCMP, with access restricted to RCMP security cleared contractor personnel only and the RCMP client. The FIPS 140-2 compliant portable storage device must be delivered by-hand or shipped by an approved courier to the contractor's location. Sensitive RCMP information shall not be transmitted to or from any external email address.

2. The password for the portable storage device is to be provided verbally, either in person or by telephone to RCMP security cleared contractor personnel only.

3. IF electronic processing of Protected A or B RCMP information is required, the contractor must ensure the information is:
   - encrypted while at rest
   - encrypted while in transit; and
   - access controls are implemented.

   Note: Advanced Encryption Standard (AES) Algorithm with key lengths of 128, 192 and 256 bits is approved for encrypting Protected A and B information.

**Mobile Users**

1. Use only RCMP-issued equipment approved for mobile use.

2. Use an approved full-disk encryption method on laptop computers and encrypt sensitive information when not in use

3. Remove your credential/authentication token and keep it on your person, when the technology it is used with is left unattended.

4. Ensure that the laptop and/or storage media containing sensitive information are stored in an authorized security container if the information is not encrypted. See AM ch. XI.3., sec. H

**Telephony**

5. All voice communication by any cellular or mobile telephone must be restricted to non-sensitive information, unless the phone is specifically accredited and issued for sensitive information.

6. Use of RCMP supplied smartphones/cellphones are restricted to RCMP employees, authorized organizations and their agents working on behalf of the RCMP, and authorized organizations and their agents.

7. RCMP supplied smartphones/cellphones are only authorized to process up to and including Protected A information on the corporate workspace side for the purpose of RCMP business.

8. Only RCMP supplied external peripheral devices may be used externally with a RCMP supplied smartphone.

**Printing, Scanning, and Photocopying**

9. If electronic RCMP Protected information has to be printed / scanned, the contractor must have additional/dedicated computer(s), printer(s)/scanners. This equipment must not be connected to the local area network nor the Internet. This computer(s) will require RCMP approved disk drive encryption.

**Storing**

10. If required, backup of RCMP Protected A or B information is subject to the same security guidelines (encryption and access controls) as is the live information.

11. Electronic records must be destroyed according to ITSG-06 Clearing and Declassifying Electronic Data Storage Devices (refer to https://www.cse-cst.gc.ca/en/node/270/html/10572 for further into). Protected information is to be cleared using the following options:

    - Media containing PROTECTED government information can only be re-used after all data areas of the media have been alternatively overwritten with any character and its complement (e.g. binary 1s then binary 0s) for a minimum of three times.
    - Media containing PROTECTED government information that are not overwritten to the satisfaction of the RCMP are to be destroyed in accordance with RCMP approved methods (approved metal-destruction facility, incineration, emery wheel or disk sander, dry disintegration, pulverizing or smelting).

12. All RCMP supplied storage devices used throughout the duration of this contract must be returned to the RCMP immediately upon contract termination.

**Personnel Security Requirements**

**RCMP Facility Access, Level I, II, III & IV**

For contractors who only require access to an RCMP facility and will not have access to protected or classified information, systems, assets and facilities. In this scenario, the RCMP wishes to conduct local law enforcement checks only. For PWGSC procurement purposes, this should be identified in the contractual documents.

*Contractor personnel must submit to local law enforcement verification by the RCMP, prior to admittance to the facility* or *site. The RCMP reserves the right to deny access to any facility* or *site or part thereof to any contractor personnel, at any time.*

When the RCMP requires Facility Access Level 1 or 2; the successful Bidder, Contractor will submit the following to the RCMP:

1. Form TBS 330-23
2. Copy of Government issued, signature bearing photo Identification (Front and Back)

When the RCMP requires Facility Access Level 3 or 4; the successful Bidder, Contractor will submit the following to the RCMP:

1. Form TBS 330-23
2. Form TBS 330-60

3. Copy of Government issued, signature bearing photo Identification (Front and Back)
4. Two sets of fingerprints

The RCMP:

1. Will conduct local law enforcement checks.
2. is responsible for escorting requirements on its facilities or sites
3. Does not require organizational or personnel security clearances for suppliers and/or contractors providing services.
4. Will complete the PWGSC Requisition Form 9200 to indicate the security requirement with no SRCL.

**RCMP Reliability Status (RRS), Secret or Top Secret Clearance**

For contractors who require access to RCMP protected information, systems, assets and/or facilities. In this scenario, the RCMP wishes to conduct all checks required for obtaining an RRS. For PWGSC procurement purposes, this should be identified in the contractual documents.

*Contractor personnel must submit to verification by the RCMP, prior to being granted access to Protected or Classified information, systems, assets and/or facilities. The RCMP reserves the right to deny access to any of the above to any contractor personnel, at any time.*

When the RCMP identifies a requirement for RRS or a security clearance; the successful Bidder, Contractor will submit the following to the RCMP:

1. Form TBS 330-23
2. Form TBS 330-60
3. Form 1020-1 (Security Interview)
4. Two pieces of Government issued, signature bearing, photo identification (Birth Certificate and Driver's licence)
5. Two sets of fingerprints
6. Working Visa (where applicable)
7. Two passport photographs

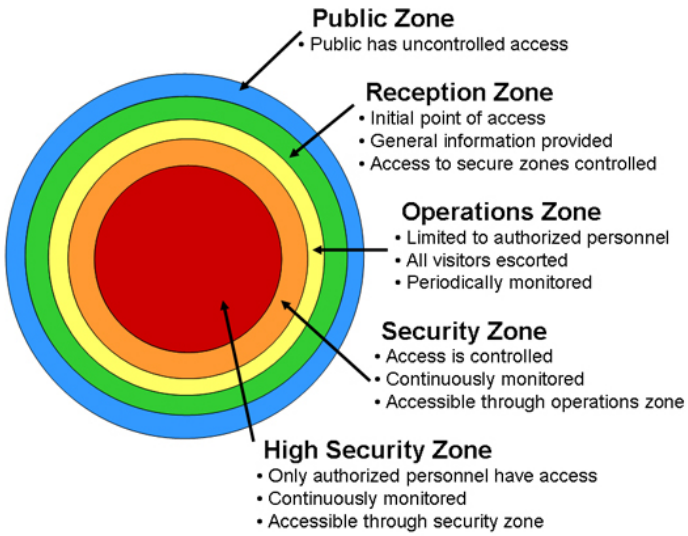
The RCMP:

1. will conduct personnel security screening checks above the Policy on Government Security requirements
2. is responsible for escorting requirements on its facilities or sites
3. will security screen any Key Senior Officials (KSOs) identified by CISD (requirement for Classified information)

## Appendix A – Security Zone Concept

The *Government Security Policy (Section 10.8 - Access Limitations)* stipulates that "departments must limit access to classified and protected information and other assets to those individuals who have a need to know the information and who have the appropriate security screening level".

The *Operational Security Standard on Physical Security (Section 6.2 - Hierarchy of Zones)* states that "departments must ensure that access to and safeguards for protected and classified assets are based on a clearly discernable hierarchy of 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.

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.