



SRCL Security Guide

RCMP Insurance Plans SRCL#: 201902673

Prepared by: Glenna Burke, Kevin Therrien
Central Departmental Security Section
Royal Canadian Mounted Police

Reviewer initials and date: ft' 1'111'1f"

Reviewer initials and date: -----

Template date: August 8th, 2017



Preamble

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

General Security Requirements

The security of the documents, records and other information that come to be in the possession of the Contractor as a result of the requirement established is of critical importance to the RCMP.

1. The Contractor must not remove or make copies of any protected information or assets from the identified work site(s).
2. The Contractor must perform all work and/or services in Canada and all the data collected, maintained, or otherwise managed must not be exchanged, linked, or provided, electronically or otherwise, to any entity beyond Canadian borders, thereby ensuring compliance with the Access to Information Act and the Privacy Act (<http://laws.justice.gc.ca>).
3. The Contractor must meet all GC security standards prior to having any information processed or stored within their facilities.
4. The Contractor must also cooperate with the RCMP or its designated party for the security review in accordance with the Security Requirements Checklist (SRCL).
5. The Contractor must cooperate with the RCMP, throughout the lifetime of the contract, for security audits of its facilities and supporting infrastructure. Note: The RCMP reserves the right to perform system scans and/or audits to validate compliance to the Departmental security requirements.
6. The Contractor must ensure any network connection is secure and meets the RCMP security requirements and standards (e.g. VPN solution meeting FIPS 140-1 level 2) and requires that all flows of information be unidirectional.
7. The Contractor must ensure that all access is protected using role based access requiring the use of identification and authentication. Roles are to be defined and associated to specific access. A sole role must be established for the creation and modification of other roles. No two individual users must be granted the same user name or password even if both individuals have common roles.
8. The Contractor must, for the RCMP, have a fully encrypted network from end to end including any sub contracts, and to the point of connectivity to them. The Contractor and any sub-contractors must meet GC's standards for level of encryption.
9. The Contractor must ensure that all data systems, connectivity and telecommunication methods, data transfers, reports, physical locations, and individuals with access to systems and/or data, and handling of all Protected information meets the Government of Canada Privacy and Security policies and legislation, inclusive of definitions and applicable documents.
10. The Contractor must ensure that all Protected 'B' information is kept encrypted while on the servers at the Contractor's location.
11. The Contractor must ensure that any exchange of information with the RCMP be performed using a 'pull method' rather than 'push method' and be transaction-based.

12. The Contractor must immediately notify the Project Authority prior to making changes to its personnel structure, locations where work is to be performed including movements within the building, Information Technology system(s), or any other changes that might impact the security of RCMP information, so that an updated Security Review can be performed.
13. 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.
14. The contractor will promptly notify the RCMP contract authority of any security incidents related to the RCMP information provided. (i.e. loss of sensitive information, accidental or deliberate.)
15. Photography is not permitted. If photos are required, please contact the Contract Authority and Departmental Security Section
16. 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
17. 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
- 18. 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)
19. 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.

Note: If, at any time during the course of the Contract, the Contractor is found to be non-compliant with respect to a security requirement that is imposed by the RCMP (via the Statement of Work, the Contract or otherwise), the Project Authority may, at their discretion:

direct that the Contractor takes such steps as the Project Authority deems necessary to be compliant with the security requirement(s), within the timeframe set by the Project Authority.

Physical Security

Information Management and Responsibilities:

- Handle all information received in confidence and take all required and necessary measures to preserve its confidentiality, integrity and availability and safeguard the information against accidental or unauthorized access, use or disclosure;
- Access to PROTECTED information and assets must be limited to persons who hold a valid RCMP Reliability Status and who have a "need-to-know". Precautions must be taken to ensure that un-cleared persons and those who do not have a need to know who may be in the proximity of information and assets, do not gain access to this information and assets either through physical access or visual oversight;
- Do not disseminate any information received or generated as part of this contract to any third party without the prior written consent of the RCMP except as required by law;
- Immediately notify the RCMP if a request is received under the *Privacy Act*, the *Access to Information Act* or other lawful authority, for information related to this contract. If requested, the contractor will endeavor to protect the information from disclosure to the extent permitted by law;
- Return to the RCMP any information that should not have been provided to it.

Security Assessment:

- Participants are jointly responsible for conducting a Security Assessment at all physical sites where processing and/or storage (hardcopy / electronic) will take place as part of this contract. This must be done in order to assess whether the required administrative, technical and physical safeguards to ensure privacy, confidentiality and integrity and availability of the information can be implemented and any revisions to the requirements based on site conditions are identified and implemented. Prior to any work being conducted as part of this contract the assessment must be agreed to and signed off by both parties.

Access Badge and Key Control:

- Access privileges to the RCMP Insurance Administration Program Area and associated rooms within must be reviewed periodically to ensure that only those employees with a need to access the program area have access.
- When an employee leaves or no longer requires access to the program area it should be removed immediately and the record of access shall be updated by the security office.
- Keys (devices such as instruments, cards, combinations and code numbers used to open and close containers or project room) shall be safeguarded, commensurate with the highest level of sensitivity of the information or assets to which they provide access. This also applies to recorded information that would allow a key to be produced.

- When a key is issued, the recipient must sign for the key. The number of the key, the location of the container it opens, and the name of the recipient shall be recorded and kept by the Company Security Officer.
- The organization's security office shall maintain a record of the dates of, and reasons for all key changes.
- Assigned combinations should be changed:
 - o At least every twelve (12) months; and
 - o When those with access to the container are transferred, released or no longer require access.
 - o When a container has been or may have been compromised, the key must be changed immediately.

Marking Information:

Organizations are required to implement the following procedures for marking information:

- For PROTECTED information, mark the word "PROTECTED" in the upper right corner of the face of the document and where required, with the letter "A" or "B" to indicate the level of safeguarding;
- Mark covering or transmittal letters or forms or circulation slips to show the highest level of classification or protection of the attachments;
- Mark all materials used in preparing PROTECTED information. Such material includes notes, drafts, carbon copies and photocopies;
- The letters used in marking should be larger than those used in the text of the document; and
- Charts, maps, drawings, etc. shall be prominently marked near the margin or title block in such manner that the marking is clearly visible when the document is folded.

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.

It is crucial to keep sensitive information secure when sending it to someone else. Sensitive information is released on a need-to-know basis only to recipients cleared for the security level.

The security of PROTECTED information and assets during transmission depends on:

- Proper packaging;
- Record while in transit;
- Record of delivery; and
- Transmission by an approved postal service or security-cleared courier.
- 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.

Reproduction:

Reproductions of PROTECTED information must be marked in the same manner as the originals.

Special precautions must be taken with the use of photocopy machines and photocopy machines dedicated to this contract must be provided. Notices concerning the proper procedures for reproduction of information shall be placed in an obvious place close to each machine. Care should be taken to ensure that original documents are not left in the machine, and all copies, including waste, are removed. At the end of the contract or when photocopy machines or hard drives are replaced all drives must be given to the RCMP.

Destruction:

The method chosen to destroy sensitive information depends on the level of sensitivity. When a paper or digital file has more than one classification or level of protection, choose the method of destruction for the highest level of sensitivity.

- Unless otherwise specified, PROTECTED A and B, of Canadian origin, may be destroyed by the organization with the approval of the RCMP.
- PROTECTED information and assets which have been authorized for destruction must be disposed of in accordance with the following:
 - It must be destroyed only by approved destruction equipment, or at a facility authorized by the RCMP;
 - Information awaiting destruction or in transit to destruction must be safeguarded in the manner prescribed for the most highly PROTECTED information asset involved;
 - PROTECTED information/assets awaiting destruction must be kept separate from other information/assets awaiting destruction;

- o An employee with a RCMP Reliability Status (RRS) must be present to monitor the destruction of PROTECTED information; and
- o Surplus copies, and waste that could reveal PROTECTED information must be protected to the appropriate level and should be promptly destroyed.

Verbal and Message Communication:

If information needs to be electronically transmitted (i.e. via e-mail), refer also to the IT Security Systems Section:

- PROTECTED information cannot be transmitted without RCMP approved encryption.
- Unprotected telephones or facsimiles are not to be used to communicate PROTECTED B or PROTECTED C information.
- When discussing PROTECTED information, be aware of your surroundings as there could be someone without the "need-to-know" in close proximity.

Security Incidents:

The contractor must immediately report any security incident to the RCMP as well as conduct a preliminary inquiry into the incident to determine all of the circumstances, including:

- What, where and when did the incident occur?
- Who reported it, to whom, and when?
- What information or asset was involved (in detail)?
- What was the security marking and description of the information or asset involved?
- Who originated the information or asset?
- When, for how long, and under what circumstances was the information or asset vulnerable to unauthorized disclosure, and to whom?
- What actions were taken to secure the information or asset and limit the damage?
- Is any information or asset lost or unaccounted for?

PHYSICAL SECURITY REQUIREMENTS**Zoning:**

- The RCMP Insurance Administration Program must be located in a clearly defined dedicated office area (refer to Information Processing Area and Information Storage Area sections) with access restricted to those employees working in the RCMP Insurance Administration Program and having the proper security clearance and need-to-know;
- The dedicated information processing area (general office) of the RCMP Insurance Administration Program must not be in a location that would require entry to it as part of a Building Code required access to exit route or provide access to another non related program area within the facility;
- The storage of hardcopy files must be located within and accessed from within the RCMP Insurance Administration Program information processing area (general office);

- The electronic storage of files must either be located on servers within the dedicated RCMP Insurance Administration Program area or located within the contractors dedicated server room.
- Access to the information processing area (general office) must be from a secured area with restricted access.

Information Processing Area (General Office):

Special care must be taken to safeguard against disclosure or unauthorized access when PROTECTED information and assets are removed from approved storage containers or file storage room:

- General:
 - o Do not leave PROTECTED information and assets unattended; and
 - o Ensure that PROTECTED information and assets cannot be viewed, or discussion of it overheard, by persons not possessing the proper security clearance and need-to-know.
- Perimeter Walls and Doors:
 - o The main information processing area (including call centre) must be located in a dedicated work area with perimeter demising walls (metal stud and gypsum board) that are full height (floor to floor);
 - o The doors to the information processing area to be solid core wood c/w hollow metal frame, acoustic seals and aluminum threshold.
 - o The perimeter demising walls and access doors (double door vestibule arrangement) must be designed to meet STC 55;
- Access control, Intrusion Detection and Monitoring:
 - o The information processing area (general office) must be equipped with an alarm system that provides 24/7 monitoring, includes full coverage motion sensors in the office area, door contacts (at all perimeter doors) and is activated and de-activated by employees working in the RCMP Insurance Administration Program;
 - o Access to the RCMP Insurance Administration Program office area must be through a dedicated vestibule arrangement with doors equipped with electronic access control.
 - o Access logs shall be made available to the RCMP.

Information Storage (Hard Copy and Electronic) Area:

- General:
 - o Access to program files must be restricted those employees working in the RCMP Insurance Administration Program and having the proper security clearance and need-to-know;
 - o The storage of hardcopy files must be located within a clearly defined dedicated file room (open shelf) or stored within containers acceptable to RCMP Departmental Security Section (DSS). Access to the file room and / containers should be from within the RCMP Insurance Administration Program information processing area (general office). The file room must not located on an exterior wall and windows (interior or exterior) are not permitted;

- o Where file servers are located with RCMP Insurance Administration Program office area they should be located within a dedicated server room designed to meet the requirements of the file storage room;
- o Where file servers are located within the contractors server facility it must be located in a dedicated server room with access restricted to those possessing the proper security clearance and need-to-know. Servers containing RCMP data must be contained within a locked server rack c/w a monitored tamper alarm.
- o The contractor must provide for a backup server facility where all RCMP Insurance Administration Program files are stored and can be retrieved within the defined recovery time. This facility should be located a minimum of 500 km away from the primary contract site. File servers located within the contractors server facility must be in a dedicated server room (area) with access restricted to those possessing the proper security clearance and need-to-know. Servers containing RCMP data must be contained within a locked server rack c/w a monitored tamper alarm.
- File Room Perimeter Walls and Doors:
 - o The Information Storage Area / Server room (if applicable) must have perimeter demising walls (metal stud and gypsum board c/w wire mesh) that are full height (floor to floor);
 - o The door(s) to the Information Storage Area / Server room (if applicable) must be hollow metal c/w hollow metal frame.
- Access control, Intrusion Detection and Monitoring:
 - o The Information Storage Area/ Server room (if applicable) must be equipped with an alarm system (separate zone from information process area) that provides 24/7 monitoring, includes full coverage motion sensors, door contacts (at all perimeter doors) and is activated and de-activated by employees working in the RCMP Insurance Administration Program;
 - o Access to the file storage room / server room (if applicable) must be through a dedicated door equipped with electronic access control c/w integrated deadbolt (deadbolt cannot be over ridden by the electronic access control)
 - o Access logs shall be made available to the RCMP.

IT Security**Appropriate Control of Protected A and B Information****Transport/Transmittal****Portable Media**

- I. If there is a requirement to send RCMP Protected A or Protected B data, 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

- I. 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 info). 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

1. All contractor and sub-contractor personnel will be required to obtain and maintain a personnel security clearance/status commensurate with the sensitivity of the work being performed throughout the life cycle of the contract (in accordance with the provisions of the SRCL) which is ERS (Enhanced Reliability Status).
2. The contractor will be responsible for advising the RCMP of any changes in personnel security requirements. For example: Cleared personnel leaving the company or no longer supporting the RCMP contract, new personnel requiring security screening and personnel requiring renewal of their personnel security screening.
3. As the supplier and its employees will have access to RCMP Protected and/or Classified information, an RCMP Clearance at the appropriate level is required.
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 contractor personnel, at any time.

When the RCMP identifies a requirement for ERS (Enhanced Reliability Status); the Contractor will submit the following to the RCMP:

1. Form TBS 330-23 (LERC version)
2. Form TBS330-60
3. Form RCMP 1020-1 (Pre Interview)
4. Copy of Birth Certificate and Driver's License
5. 2 Passport size pictures.

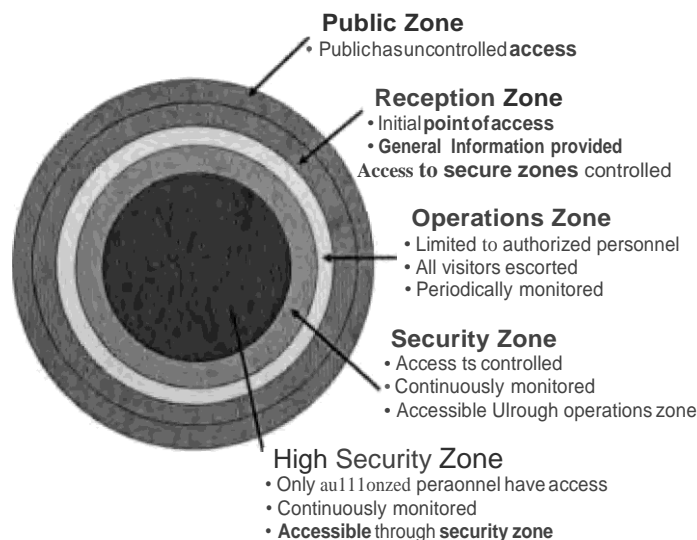
The RCMP:

1. will conduct personnel security screening checks above and beyond the security requirements outlined in the *Policy on Government Security*
2. will conduct a security interview
3. will obtain a set of fingerprints

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 GI-026, Guide to the Application of Physical Security Zones for more detailed information.