RCMP·GRC

ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

SRCL Security Guide

Standing Offer

for

The National Missing Persons DNA Program (NMPDP)

SRCL #: PSPC M7594-173247

Prepared by :
Departmental Security Section
Royal Canadian Mounted Police

Reviewer initials and date: _____

Reviewer initials and date: _____

Template date: Aug 3, 2017

Preamble

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

Given the nature of this project, the following guidelines only apply to sensitive RCMP information disseminated from the RCMP (by designated contact) to the contractor.

General Security Requirements

1. All Protected B 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 contract authority of any security incidents related to any RCMP information and/or samples provided. (i.e. loss of sensitive information, accidental or deliberate.)

4. 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.

5. The RCMP's Departmental Security Section (DSS) reserves the right to conduct inspections of the contractor's facility and provide guidance on mandatory safeguards (safeguards as specified in this document and possibly additional site specific safeguards). Inspections may be performed prior to sensitive information being shared and/or as required (e.g. if the contractor's office relocates). The intent of the inspection is to ensure the quality of security safeguards.

6. 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.

7. No work is to commence on this requirement until Security measures are approved by the RCMP Project Authority.

Physical Security

1. **Storage**: Protected information/assets must be stored in a container approved by 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. Note: The personnel working within the Operational Zone must: • possess a valid RCMP Reliability Status (RRS), or • 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

1. If Protected A or Protected B RCMP information is required to be sent electronically, one of the following options may be used:

   - It may be sent via FIPS 140-2 compliant portable storage device provided by RCMP, with access restricted to RCMP security cleared contractor personnel only and the RCMP client. The FIPS 140-2 compliant portable storage device is to be delivered by-hand or shipped by reliable courier (Note: PSPC's CIISD can provide a list of reliable courier service providers) to the contractor's location.

     NOTE: *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.*

   - It may be emailed using Secure RCMP Entrust encrypted email

2. IF any electronic processing/sending of Protected A or higher 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) Algorithms with key lengths of 128, 192 and 256 bits are approved for encrypting Protected A and B information.

3. 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.

4. Personal smartphones must not be used to process any RCMP business related activities.

5. 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 reused 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).

6. 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 hard disk drive encryption.

7. 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.

8. 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).

Personnel Security

1. All contractor personnel will be required to obtain and maintain a RCMP 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).

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 Security Clearance at the appropriate level is required.

   Prior to being granted access to Protected/Classified information, systems, assets and/or facilities, contractor personnel must submit to verification by the RCMP. 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 Contractor will submit the following to the RCMP:

   1. Form TBS 330-23 (LERC version)
   2. Any additional forms that may be required.

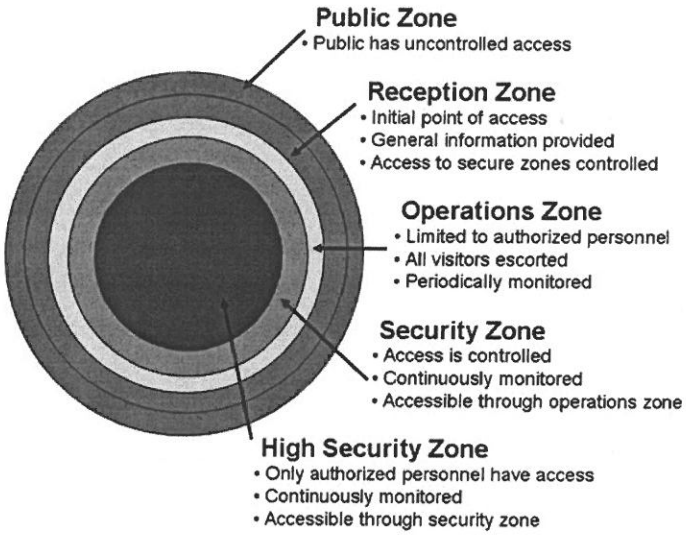
   The RCMP:

   1. Will conduct personnel security screening checks that exceed the security requirements identified from the *Policy on Government Security*.

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.