SRCL Security Guide

SRCL #: 101713

Prepared by:
Central Departmental Security Section
Royal Canadian Mounted Police

General Security Requirements

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. Physical access to RCMP facilities/sites is restricted to those specific areas required to meet the contract's objectives.

2. Before entering an operational area of an RCMP building/facility, contractors and Sub-contractors not cleared to ERS, must turn in all electronic devices, e.g. cell phones, cameras, smartphones to the reception/security desk until the person leaves.

3. Contractors must be escorted at all times when within RCMP space.

4. The contractor may not use un-screened personnel for portions of the work.

5. The contractor may not remove any Classified information or assets from RCMP properties and/or facilities.

6. The contractor may not produce, store, manufacture, repair and/or modify any Protected/Classified material or equipment on its site or premises.

7. A building access card is required for admittance to or movement within an RCMP building/facility, which must be worn and visible at all times.

IT Security

1. No sensitive information, Protected A or higher, shall be electronically transmitted outside of RCMP networks or processed at the contractor's site.

2. No sensitive electronic information or assets, Protected A or higher, shall be removed from RCMP networks or property.

3. 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.

4. Individuals must not use privately-owned technology to join, bridge, or participate with RCMP networks in any way on RCMP premises including creating a network or access point.

5. All contract work is to be done on RCMP premises with escorted continuous monitoring.

6. Only contractors who have a RCMP ERS security clearance are permitted to use a personal cell phone (with prior permission) on RCMP premises, however communication;
    a. must be restricted to non-sensitive information;
    b. must not be used to conduct RCMP business and;
    c. must not be connected to RCMP communications technology at any time.

7. Any conference/video calls involving the discussion of RCMP information must be conducted using an RCMP authorized video conferencing medium approved for the level of information being transmitted.

Personnel Security

1. All contractor and sub-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.

When the RCMP requires **Facility Access Level II**; the Contractor will submit the following to the RCMP through the RCMP online security portal:

1. TBS Security Screening Application and Consent Form
2. Copy of Government Issued Photo Identification (Driver's License Front and Back)

The RCMP:

1. Will conduct personnel security screening checks above the Policy on Government Security requirements.
2. Is responsible for escort requirements on it facilities or sites.