RCMP ROYAL CANADIAN MOUNTED POLICE

Contract Security Guide

M7594224467

Departmental Security - NHQ Ottawa

SRCL#M7594224467

Table of Contents

1. Introduction

1.1. Preamble

1.1.1. All contract statements and appendices within this SRCL Security Guide are only applicable to this contract.

1.1.2. All contractors employed on this contract must support and maintain the security environment of the Royal Canadian Mounted Police (RCMP) by complying with the requirements described in this document. More comprehensive security obligations will be provided at the Request for a Proposal phase if applicable. This security guide only covers services or personnel storing or processing unclassified information.

1.2. Definitions

Compromise	A breach of government security which includes, but is not limited to: • Unauthorized access to, disclosure, modification, use, interruption, removal, or destruction of sensitive information or assets, causing a loss of confidentiality, integrity, availability or value; • Any action, conduct, threat or gesture of a person toward an employee in the workplace or an individual within federal facilities that caused harm or injury to that employee or individual; • Events causing a loss of integrity or availability of government services or activities.
Contractor	The entity (can include one or more natural persons, corporations, partnerships, limited liability partnerships, service providers, vendors, etc.) delivering the services to the RCMP and its partners. It is the entity approved and referenced as the 'contractor' on the resulting contract.
End User	A person who uses an application or system for its primary purpose, e.g. the ultimate user, in contrast to system engineers, developers, administrators.
Information Spillage	Refers to incidents where an Information Asset is inadvertently placed on an Asset or System that is not authorized to process it (e.g. ITSG-33, IR-9).
Metadata	Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).
Organizational data	Information or data created for, collected by, under the custodianship of, or owned by the RCMP in any format, including but not limited to text, audio, video, or image, software, and related metadata.

Personal Information	Information about an identifiable individual and recorded in any form, as defined in the Privacy Act, Section 3. Examples include, but are not limited to the information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual.
Project Authority	The entity responsible for the management of the contract. Any changes to the contract must be authorized in writing by the Project Authority, and the contractor must not perform work in excess or outside of the scope of the contract based on verbal or written requests or instructions from anyone other than the Project Authority.
Protected Information or Assets	When unauthorized disclosure, destruction, interruption, removal or modification to information or asset could reasonably be expected to cause injury to non-national interest.
Record	Any hard copy document or any data in a machine-readable format containing Personal Information.
RCMP Security Authority	The entity within an organization who is authorized to approve contract security and retains the Security Requirements Checklist (SRCL) signing authority.
Security Clearance	The necessary security clearance, such as Secret and Top Secret Clearance, designated by Departmental Security of the RCMP, which may include some or all of the security screening steps listed in the appropriate Security Clause.
Security Event	Any event, omission or situation that may be detrimental to government security, including threats, vulnerabilities and security incidents.
Security Incident	Any event (or collection of events), act, omission or situation that has resulted in a compromise. Examples of cyber security incidents: Active exploitation of one or more identified vulnerabilities, exfiltration of data, failure of a security control, breach of a cloud-hosted or managed Government of Canada (GC) service, etc.
Security Screening	Refer to the definition in Appendix A – Definitions, of the Treasury Board's Standard on Security Screening.
Sensitive	An information management security category that is used to identify information or other assets that, if compromised, would reasonably be expected to cause an injury in either national (classified) or non-national (protected) interest. Also refer to the definitions for classified and protected.
Sub-contractor	Any person to whom the contractor subcontracts the performance of the contractor's services, in whole or in part.
Sub-Processor	Any a natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller or contractor.

Telework	An agreement between a contractors' employee and the Project Authority to carry out some or all of their work duties from a remote location. Telework requires the completion of a telework agreement between the contractor and the Project Authority.
Unclassified Information	Non-sensitive information that is created and owned organizationally and accessible to all authorized individuals. Unauthorized disclosure would cause no injury to national and non-national interest.

2. General Security Requirements

2.1. All organizational data, including hard copy documentation, or other assets for which the RCMP is responsible will be shared with the contractor through pre-approved processes.

2.2. The information disclosed by the RCMP will be administered, maintained, and disposed of in accordance with the full contract.

2.3. The contractor will promptly notify the RCMP Security Authority of any security incidents related to organizational data or personnel in their employ.

2.4. External IT assets and devices are restricted in RCMP facilities. Visitors attending RCMP premises with non RCMP IT equipment are required to turn in all electronic equipment upon arrival to the reception/security desk until departure.
Note: An exception may be granted when valid ERS clearance is present with authorization from the Project Authority. You may be required to complete a form for property security to review.

2.5. Photography is not permitted within RCMP facilities. If photos are required, please contact the Project Authority and Departmental Security.

2.6. The contractor is not permitted to disclose any organizational data or ancillary information provided by the RCMP, to any sub-contractors or sub-processors without RCMP Security Assessment and Authorization (SA&A).

2.7. The RCMP's Departmental Security reserves the right to conduct inspections and/or security review of the contractors' facility(ies) and/or personnel work location(s) and provide direction 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. In the event that the contractor's office relocates). The intent of the inspection(s) is to maintain the robustness of the required security safeguards.

2.8. All organizational data must be protected through cryptographic means. Cryptographic algorithms, cryptographic key sizes and crypto periods in use must align with the Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information - ITSP.40.111 or subsequent versions, accesible on the Canadian Centre for Cyber Security, Cyber security guidance website.The contractors' personnel security clearance requirements will be based on the expected roles and access to GC data and systems. When needed, a Security Classification

Guide will be added to this Security Guide to clearly identify personnel security clearance requirements.

2.9. The work locations of all contractor personnel are to be clearly stated in Appendix B - Security Classification Guide and Statement of Work (SOW). The contractor must regularly report on the location of work including employees telework locations and the number of days worked. If the location of work is expected to change through the life of the contract this is also required to be explicitly stated. Work locations can include: (i) on-site at RCMP facilities, (ii) Telework or (iii) a hybrid of the two. The RCMP must be notified of any change in work location that is not indicated in the Classification Guide and SOW as it will require contract review and approval. Telework must follow the guidance in the section on Telework Management. All requirements outlined in Appendix C – RCMP Guidelines for Telework Location must be adhered to during Telework.

2.10. Prior to the authorization of a telework location, all security safeguards or mitigations identified as part of an RCMP security assessment must be adhered to.

2.11. Telework must be performed in Canada. Exceptions for Telework outside of Canada may be permitted from Five Eyes countries with an RCMP security assessment and written RCMP approval from the Chief Security Officer (CSO) or delegate. Security controls and requirements will be identified during the security assessment for each work location.

3. Physical Security Controls

3.1.1 The shipping of firearms are governed by *Regulations* made under the *Firearms Act.* The Regulations governing receving firearms from manufacturers is the ***Storage, Display and Transportation of Firearms and Other Weapons by Businesses***. Under this program, the firearms will be classified as **Prohibited Handguns**, therefore we will need to follow Section 12 of the Regulation:

Transportation of Restricted Firearms and Prohibited Handguns

12 (1) A business may transport a restricted firearm or a prohibited handgun only if

(a) it is unloaded; and

(b) it is in a container

(i) that is made of an opaque material and is of such strength, construction and nature that it cannot be readily broken open or into or accidentally opened during transportation, and

(ii) that, subject to subsection (2), does not have any markings on its exterior that could indicate that a weapon, a prohibited device or ammunition is in it; and

(c) when it is in a container described in paragraph (b) that is in an unattended vehicle,

(i) if the vehicle is equipped with a trunk or similar compartment that can be securely locked, the container is in that trunk or compartment and the trunk or compartment is securely locked, and

(ii) if the vehicle is not equipped with a trunk or similar compartment that can be securely locked, the vehicle, or the part of the vehicle that contains the container, is securely locked and the container is not visible from outside the vehicle.

(2) Subparagraph (1)(b)(ii) does not apply if

(a) the only marking on the exterior of the container that could indicate that a weapon, a prohibited device or ammunition is contained in it is a name or address; or

(b) the container and its contents are being imported into Canada or exported from Canada.

4. Information Technology (IT) Security Controls

4.1. Flow-Down of Security Obligations

4.1.1. The security obligations apply to the contractor and to any sub-contractor and/or sub-processors to the extent applicable. When applicable, the contractor is accountable to ensure their sub-contractors and/or sub-processors comply with these security obligations.

4.2. Use of Sub-Contractors, Sub-processors and/or Sub-sub-processors

4.2.1. The contractor must provide a list of sub-contractors, sub-processors and sub-sub-processors that could be used to perform any part of the work in providing the RCMP with the Service or that are related to an investigation of a security event or Incident that may have an impact on or to RCMP organizational data. The list must include the following information:

a) The name of the sub-contractors, sub-processors and/or sub-sub-processors; and
b) The identification of the work that would be performed or service provided by the sub-contractors, sub-processors and/or sub-sub-processors; and
c) The location(s) where the sub-contractors, sub-processors and/or sub-sub-processors would perform the work.

4.2.2. The contractor must provide a list of sub-contractors, sub-processors and/or sub-sub-processors within ten days of the effective date of the contract.

4.2.3. The contractor must provide the RCMP notice of any new sub-contractors, sub-processors and/or sub-sub-processors at least 14-days in advance of providing that sub-contractors, sub-processors and/or sub-sub-processors with access to any organizational data.

4.3. Roles and Responsibilities for Security

4.3.1. The contractor must clearly delineate the roles and responsibilities for the security controls and features of the solution between the contractor and the RCMP. This includes, at a minimum, the roles and responsibilities for:

a) Account management;
b) Boundary protection;

c) Asset and information system backup;
d) Incident management;
e) System monitoring; and
f) Vulnerability management.

4.4. Telework Management

4.4.1. The work locations of all contractor personnel are to be clearly stated in the Classification Guide and Statement of Work (SOW). The contractor must regularly report on the location of work including employees telework locations and the number of days worked. If the location of work is expected to change through the life of the contract, this is also required to be explicitly stated. The RCMP must be notified of any change in work location that is not indicated in the Classification Guide and SOW as it will require contract review and security approval.

4.4.2. Work locations can include: (i) on-site at RCMP facilities, (ii) Telework or (iii) a hybrid of the two. Where the location of work is hybrid, the Project Authority must provide a detailed schedule indicating the dates where the personnel will be working in which category. Telework includes any location outside of an RCMP facility. Telework must be performed in Canada, but may be permitted from Five Eyes countries with an RCMP security assessment and written RCMP approval from Chief Security Officer (CSO) or delegate. Regardless of the remote work location, all security guidance within this document apply. This includes work at the contractors' facility(ies), a contractor personnel's residence, or any other remote work location.

4.4.3. When the use of RCMP-provided equipment is indicated on the SRCL, the Project Authority and Contractor must:

a) Manage and monitor remote access by the contractor to RCMP systems and/or organizational data;
b) Conduct all duties throughout the contract using the provided equipment;
c) Issue standard RCMP equipment for remote work, this includes an RCMP imaged laptop with approved full-disk encryption;
d) Utilize multi-factor authentication with standard RCMP issued credentials for all secure access requirements (e.g. VPN access);
e) Ensurethe contractor understands and acknowledges their responsibilities and complies with the Acceptable User Practices for RCMP Information Technology;Ensure RCMP equipment remains within the specified work locations at all times.

4.4.4. When the use of RCMP-provided equipment is not indicated on the SRCL, the contractor may use their own equipment provided it abides by the security requirements in the section on Endpoint Protection.

4.5. Endpoint Protection

4.5.1. Where end points are provided by the contractor, the contractor must implement, manage, and monitor security-hardened endpoints with active host-based protections to prevent against malware, attacks and misuse in accordance with industry recognized configuration guidelines such as those found in in National Institute of Standards and Technology (NIST) 800-123 (Guide

to General Server Security), the Center for Internet Security (CIS) Benchmarks or an equivalent standard approved by the RCMP in writing.

4.6. Cryptographic Protection

4.6.1. Contractor personnel must:

a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods;

b) Use cryptographic algorithms and cryptographic key sizes and crypto periods specified in Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information – ITSP.40.111 or subsequent versions, accessible on the Canadian Centre for Cyber Security website.

4.7. Data Protection

4.7.1. When the use of RCMP-provided equipment is required, all duties assigned to the contractor are required to be completed using the provided equipment and follow RCMP guidance on Telework Management. Contractor personnel are not permitted to use any non-approved software, services or equipment not provided by the RCMP unless otherwise stated in writing. If the use of RCMP-provided equipment is not required, the contractor may use their own equipment provided it abides by the security requirements in the section on Endpoint Protection.

4.7.2. Organizational data is not to be stored on cloud services unless the service has been issued an Authority to Operate (ATO) by RCMP Departmental Security. The Project Authority is responsible for ensuring an ATO has been issued and all conditions are being followed throughout the life of the contract.

4.7.3. Any backup of organizational data is subject to the same security guidelines for encryption and access controls as the primary data source.

4.7.4. Electronic records and media devices must be sanitized and/or destroyed according to IT Media Sanitization - ITSP.40.006 or subsequent versions, accesible on the Canadian Centre for Cyber Security website.

4.7.5. It is not permitted for either the contractor and/or contractor personnel to make any copies of databases or any part of those databases containing organizational data outside of regular service resilience capabilities and within RCMP approved regional spaces or zones.

4.7.6. The contractor and/or contractor personnel must not move or transmit organizational data at rest outside of agreed upon service regions except when approval is obtained from RCMP.

4.7.7. The contractor must:

a) Implement end-to-end encryption for all protected data in transit. All encryption of data-in-transit must meet the requirements in ITSP.40.111 Cryptographic Algorithms for

UNCLASSIFIED, PROTECTED A, and PROTECTED B Information – ITSP.40.111, or subsequent versions, accesible on the Canadian Centre for Cyber Security website;

b) Implement encryption of data at rest for all services hosting organizational data, including any and all metadata or logs derived from or related to organizational data, where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, as specified in Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information – ITSP.40.111, or subsequent versions, accessible on the Canadian Centre for Cyber Security website;

c) Implement security controls that restrict administrative access to organizational data, including any and all metadata or logs derived from or related to organizational data and systems by the contractor and provides the ability to require the approval of RCMP before they can access organizational data to perform support, maintenance, or operational activities.

d) Take reasonable measures to ensure that contractor personnel do not have standing or ongoing access rights to organizational data without a need-to-know, including resources that provide technical or customer support based on approval from the RCMP.

e) Prevent any contractor personnel from holding credentials that allow that personnel to delete, modify or copy organizational data, unless that person has been cleared by the RCMP to the appropriate level deemed required by the RCMP.

4.8. Data Transport/Transmittal

4.8.1. If there is a requirement to transport organizational data, it must be transported using a FIPS 140-2 Level 2, or higher, compliant portable storage device provided by the RCMP. Access to this device must be restricted to appropriately security cleared contractor personnel only, as well as the RCMP client. The FIPS 140-2 Level 2 compliant portable storage device must be delivered by-hand or shipped in accordance with the section on Physical Security Controls - Transport/Transmittal of Physical Assets.

4.8.2. The password for the portable storage device is to be provided via out-of-band means, either in person or by telephone to appropriately security cleared contractor personnel only.

4.8.3. Where there is a requirement to transmit organizational data, including any and all metadata or logs derived from or related to organizational data it must be done in a secure manner including the implementation of encryption for data in transit as outlined in the section on Cryptographic Protection.

4.9. Data Disposition and Returning of Records

4.9.1. The contractor must crypto-shred resources (for example, equipment, data storage, files, and memory) that contain organizational data and ensure that previously stored data cannot be accessed by other customers after it is released. This includes all copies of organizational data that are made through replication for high availability and disaster recovery. The Contractor's disposal or reuse of resources must be aligned with one of the following:

a) IT Media Sanitization - ITSP.40.006 or subsequent versions, accesible on the Canadian Centre for Cyber Security website; or
b) Guidelines for Media Sanitization - NIST SP 800-88; or
c) Upon request of the RCMP, the contractor must provide a document that describes the contractor's process for disposal or reuse of resources.

4.9.2. The contractor must provide the RCMP with confirmation through a letter of attestation or log entries, that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once the RCMP discontinues its use of the Services. The RCMP may require proof that encryption keys have been destroyed or that data has been successfully crypto-shredded to prevent the recovery of data.

4.9.3. In the event of contract termination or when otherwise requested by the RCMP, the contractor must:

a) Ensure all data protection and security controls remain in place, as detailed in the Security Guide during the period where the RCMP is recovering organizational data; and
b) Provide the RCMP with access to its organizational data for a period of time that enables the RCMP to recover all organizational data from the contractor.

4.10. Security Event Reponse

4.10.1. Government of Canada Cyber Security Event Management Plan (GC CSEMP) defines a Security Event as: "Any event, act, omission or situation that may be detrimental to government security, including threats, vulnerabilities and incidents". In light of this, the contractor must alert and promptly notify the RCMP Security Authority (via phone and/or email) of any compromise, breach or of any evidence such as:

a) A security event;
b) A security malfunction in any asset;
c) Data spillage;
d) Irregular or unauthorized access to any asset;
e) Large scale copying of an information asset; or
f) Any other irregular activity identified by the contractor that leads the contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function.

4.10.2. If the contractor becomes aware of or determines that a compromise or breach of security has occurred (for example,leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access) while personal information or organizational data is handled by the contractor, the contractor is responsible to:

a) Notify the RCMP Security Authority of the security event within 24 hours;
b) Investigate the security event and provide the RCMP with detailed information about the security event; and
c) Take reasonable steps to mitigate the cause and to minimize any damage resulting from the security event.

4.11. Printing, Scanning, and Photocopying

4.11.1. Printing, scanning, and/or photocopying sensitive organizational data must be pre-authorized by the RCMP.

4.11.2. When printing/scanning/photocopying is authorized, the contractor must:

a) Have additional/dedicated printers/scanners/photocopiers that are not directly connected to any network including the internet. Dedicated local connections of these devices to the contractors end-point(s) is acceptable;
b) Align with the requirements identified in the Physical Security Controls sections on Storage, Production of Hard Copy Information or Other Assets and Destruction; and
c) Sanitize and/or destroy printing/scanning/photocopying devices (such as multi-function devices, printers, copiers) according to IT Media Sanitization - ITSP.40.006 or subsequent versions, accesible on the Canadian Centre for Cyber Security website.

4.12. Identity and Access Management

4.12.1. When the use of RCMP equipment is required, contractor personnel will be assigned RCMP IAM credentials enabling them to access RCMP assets. RCMP IAM credentials are only to be used in the course of executing the tasks outlined in contracting documentation and are to be revoked at the completion of this contract.

4.13. Security Assessment and Authorization

4.13.1. Before any solutions developed in whole or in part by contractors are moved into a production environment, an Interim Authority to Operate (IATO) or full Authority to Operate (ATO) must be granted. Obtaining an I/ATO requires a security assessment as part of the Security Assessment and Authorization (SA&A) process, which can be initiated by contacting RCMP Departmental Security.

4.14. Termination

4.14.1. The Contractor must have implemented a documented termination or change of status procedure for personnel. The procedure, at a minimum, must include:

a) Notification of Termination to the Project Authority within the same day of termination;
b) Removal of information system access within same day of termination;
c) Terminate and/or revoke any authenticators and/or credentials associated with the individual within 24 hours;
d) Conduct exit interviews that include a discussion of items identified in the TBS Standard on Security Screening and any related provisions of the Industrial Security Program;
e) Submit 330-47 Security Briefing Form for termination of contractor's security clearance;
f) Retrieve all security-related RCMP information system-related property, including access cards within 24 hours; and
g) Retain access to RCMP information and information systems formerly controlled by terminated individual.

4.14.2. Contractor personnel, upon termination of the contract for any reason, are required to return to the Project Authority all RCMP issued devices including, but not limited to:

a) Laptops;
b) Cellular Phones;
c) USB Drives; or
d) Smart Cards

5. Personnel Security Controls

5.1. All contractors working for, or hired by the RCMP require a valid security status/clearance level. If the contractor personnel will have access to RCMP sensitive information, the required RCMP clearance or RCMP-approved equivalency* must be at the appropriate level. Contractor personnel must submit to verification by the RCMP, prior to being granted access to sensitive information, systems, assets and/or facilities. The RCMP reserves the right to deny access to any of the contractor personnel, at any time. In the case of an Incident, security or otherwise, the RCMP has the right to deny or suspend access to RCMP locations, services and or data if situations warrant this action, pending review of the incident.

5.2. When the RCMP identifies a requirement, for Facility Access (FA2), they will direct the contractors to the RCMP online portal for their completion of the clearance forms. **FA2 has been determined to be the level required for on site training or certifications with technical escort.**

5.3. All contractor and sub-contractor personnel must maintain their 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).

5.4. Personnel security clearance/status must be in place prior to any work commencing on the requirement.

5.5. When unscreened personnel are required, the roles must be identified and pre-approved by the RCMP in the Security Requirements Check List (SRCL) once the successful vendor is chosen.

5.6. 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.

5.7. The RCMP will conduct personnel security screening checks that exceed the security requirements identified in the Policy on Government Security.

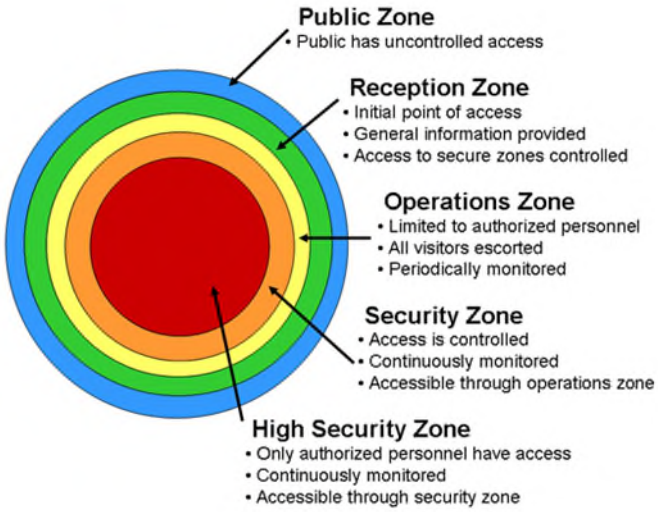
5.8. The RCMP reserves the right to increase or change the levels required if they deem appropriate, once the job roles are clearlydefined.

**Security Status/Clearance equivalencies require written RCMP approval from Chief Security Officer (CSO) or delegate.*

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 personnel and valuable assets. For more detailed information, refer to RCMP Guide G1-026, Guide to the Application of Physical Security Zones.

Appendix B – Security Classification Guide

This table is to be completed by the Project Authority when required by Departmental Security. It is important to provide as much detail as possible in the table as it forms a decision aid for the assignation of security clearance levels (for example, it is useful to include information such as the resources work location, systems they will have access to and the privilege access they may have).

In some cases, it may be possible to reuse information from the Statement of Work (SOW) associated with the contract.

When completing this table leave the Clearance Level column blank, that column will be completed by Personnel Security contracts specialists.

Role/Function	Type of Data Accessed	Work Location (Include city if outside of Canada)	Role Description and Details	Clearance Level
Trainers	*No access to PROTECTED info*	*On site Ottawa/Regina*	- *Training on the pistols* - *Certification and re-certification*	FA2 with escort

Appendix C – RCMP Guidelines for Telework Location

C.1. RCMP Guidelines for Telework Location are specific to this contract only.

C.2. Access controls must be implemented to restrict access to information to those with a bona fide "need to know".

C.3. Contractor personnel must take reasonable care to protect sensitive organizational data information and assets against unauthorized disclosure, loss, theft, fire, destruction, damage or modification.

C.4. Telework site(s) identified within the contact are subject to security review and/or inspection at any time by an RCMP representative to ensure all controls are in compliance for safeguarding of sensitive organizational data and assets.

C.5. The contractor and contractor personnel will promptly notify the RCMP Security Authority of any unauthorized use or disclosure of the information exchanged under this contract and will provide the RCMP with details of the unauthorized use or disclosure.

C.6. If the nature or scope of the work changes, the contractor must promptly notify the RCMP Security Authority, who will jointly with the contractor, review and determine appropriate security mitigations.

C.7. The RCMP Security Authority is the first point of contact to provide contractors advice and guidance on any security policy requirements and controls.

Work Paperless

C.8. Project Authority must implement paperless work options for contractor personnel.

C.9. Sensitive organizational data must be encrypted at rest and while in transit.

a. Full disk encryption is required on all devices processing sensitive organizational Data.

b. All sensitive organizational data must be encrypted at minimum with Advanced Encryption Standard (AES) Algorithm with key lengths of 128 (AES-128).

C.10. Multifactor authentication is required to access sensitive organizational data.

C.11. Use of personal storage or peripheral devices (USB devices, cell phones, monitors, printers, scanners, web cam, headset, etc.) is prohibited for accessing and processing organizational data.

C.12. When authorized, only RCMP approved and issued portable storage media (USB drive, SD cards, CD/DVD, etc.) is permitted.

C.13. When required to email or transmit sensitive data, the contractor must ensure the information is encrypted and uses an RCMP approved and authorized service.

C.14. When transporting sensitive hardcopy information and assets in any form to and from a telework location do not make any unnecessary stops between secure locations. Never leave RCMP information and assets in any form unattended, lock up all paper media or devices containing RCMP data and lock doors when not present at the telework location. Never leave paper media or devices containing RCMP organizational data in a vehicle.

C.15. Discussing or sharing sensitive organizational data over non-RCMP approved audio or video conferencing is prohibited.

C.16. All virtual meetings between the RCMP and the contractor held throughout the course of the contract will use a videoconferencing solution authorized for discussion of sensitive organizational data. The RCMP will initiate all videoconferencing sessions, and will provide the link to the videoconference to the contractor.

C.17. The contractor may be required to install the corresponding videoconferencing client on their endpoints.

C.18. Information Technology (IT) equipment processing sensitive organizational data when not in use must be stored out of sight and in a locked room, or locked container (e.g. desk drawer, box, filing cabinet) for which the contractor personnel controls access at all times.

Environment / Workspace Control

C.19. Contract personnel must:

a. Conduct work within a dedicated space which can be secured from oversight and overhearing by co-habitants and windows.

b. Be aware of the surroundings and ensure no sensitive organizational data in the background will be transmitted by video or audio.

C.20. All sensitive discussions must be safeguarded by:

a. Only using approved equipment and software.

b. Using headsets for audio and a work space secure from oversight or in an enclosed room that is both secured from overhearing and oversight by co-habitants and windows.

c. Only activating web cameras when in use.

d. Knowing how to mute the microphone and visually block the camera quickly if required.

e. Not discussing sensitive organizational data above Protected B.

f. Ensure mobile devices are left outside of areas where sensitive discussions are occurring.

g. Turn off wireless devices with a voice transmission capability or physically disable the microphone when attending a meeting at which sensitive organizational data is being discussed.

C.21. Not discussing sensitive organizational data on personal telephones, or personal equipment/software.

Additional Requirements When Using RCMP IT Equipment

C.22. When using RCMP IT equipment, contractor personnel must:

a. Read and sign the Acceptable User Practices for RCMP Information Technology; and
b. Follow RCMP IT and security policies and standards.

Termination / Expiration of Contract

C.23. Upon termination or expiration of any contractor personnel, the contractor must notify immediately the RCMP Project Authority, retrieve all RCMP IT equipment and any RCMP related information, and submit them to RCMP Project Authority for disposal or removal of RCMP contract related information.