Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Canada

Contract Security Requirements – Protected B

1. INTRODUCTION

This document outlines the IT Security requirements that the Contractor must meet prior to the processing of sensitive data up to and including the level of *Protected B*. In absence of a formal Threat-Risk Assessment (TRA) and due to the IT portion of the Security clearance being contract specific, the intent of this document is to state the minimum safeguards required by the Contractor in order that the processing of sensitive information be approved by the Public Works and Government Services Canada's Canadian Industrial Security Directorate (CISD).

Security is based upon layers of protection; that is, in order for the requirements of the IT Security (ITS) to effectively safeguard the information , they must be preceded and supported by other aspects of security and the associated policies. The physical, personnel and information security safeguards in accordance with the Policy on Government Security and ITS related Standards must exist *prior* to the implementation of ITS safeguards.

2. MANDATORY PREREQUISITES

2.1 PWGSC Validation for Physical Security

The application of the security safeguards listed in this document is based on the *mandatory requirement* that the physical premises have been inspected by the CISD, PWGSC. The Departmental Security Officer's (DSO) office will validate the certification and notify the IT Security Coordinator.

2.2 Personnel Security

All personnel who have access to the material being processed must hold valid Government of Canada security clearance at the appropriate level (dictated by the sensitivity of the material) and have the *"need to know"*.

All Contractor personnel handling Government of Canada sensitive information must attend a training/briefing session coordinated and delivered by the Treasury Board Secretariat DSO, IT Security Coordinator.

2.3 Authorization and Access Control

The Contractor must provide the Treasury Board Secretariat IT Security Coordinator with a list of all individuals who have access to the sensitive information being processed for the Department, along with Contractor current policies and procedures for adding individuals to the environment and the process followed when an individual is removed from the environment.

In following the 'principle of least-privilege', Contractor must provide only the minimum access required for individuals to perform their duties.

2.4 Information Security

All hard copy documents and other media formats must be handled and transported in accordance with Government of Canada guidelines. All hard copy documents and other media will be marked with the appropriate security classification as provided by Treasury Board Secretariat. Any covering letter, transmittal form or circulation slip will be marked to indicate the highest level of classification of the attachments.

Transportation of information associated with this Contract into or out of the physical premises mu st adhere to RCMP G1-009 *"Transport and Transmittal of Protected and Classified Information"*. Contractor personnel may only transport documents associated with this Contract into or out of the WPS Protected B physical domain with the approval of the Treasury Board Secretariat's DSO.

2.5 Security Policy Compliance Monitoring

On a frequency to be determined by the Departmental Security Officer or the IT Security Coordinator, the Treasury Board of Canada Secretariat retains the right to conduct inspections of the Contractor's facility to ensure compliance with Government of Canada standards and policies with respect to the handling, storage and processing of sensitive information.

3. MINIMUM SECURITY REQUIREMENTS (DETAILS)

3.1 Physical Security

Company must provide and/or demonstrate proof of:

- Brief description of the organization's role and facility
- Signed Company Security Orders
- Materia1 control log for Protected information and assets
- Visitor control log for Protected information and assets
- Detailed signed floor plan identifying the reception zone and the operation zone; plan mu st include all entries (doors and windows) and the location of all equipment being used to produce, store, destroy and/or transmit data
- Pictures of zones, doors, windows, cabinet, shredder and IT equipment
- RCMP approved containers for storing information at the protected A and B levels
- RCMP approved destruction equipment, or the name of a shredding company that is cleared to the appropriate level
- An appropriately security cleared cleaning organization, or cleaning done under supervision during regular working hours

3.2 Personnel Security

- All individuals must hold a valid reliability status or higher
- The maintenance of this status is required for the duration of the contract

3.3 **IT Security**

- Any loss or theft of PROTECTED information must be reported by the Contractor to the Project Authority within 2 hours of detection.
- Any computers used to store and/or process PROTECTED information shall be located in a space that meets the requirements of an Operations Zone as defined in the Treasury Board 's Operational Security Standard on Physical Security.
- If PROTECTED information is stored or processed on portable storage devices such as USB flash drives, the information must be protected by a strong password and encrypted using a product that meets Government of Canada (GC) encryption standards as defined in ITSA-11E CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within GC.
- When sending PROTECTED B information electronically via email or other electronic exchange, it must be protected by a strong password and encrypted using a product or service that meets GC encryption standards as defined in ITSA-11E CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within GC.
- All PROTECTED information in the Contractor's custody shall be stored on physical computers and storage media in their custody and located in Canada only. The use of third-party cloud services (e.g. Google Drive, Dropbox) to store PROTECTED information is prohibited.
- On all computers used to store and/or process PROTECTED information:
    - Current antivirus software must be installed and maintained with the most current virus definitions and signatures;
    - Operating System (OS) must be a vendor-supported OS (i.e. current security patches must still be available and the product not have reached end of life) and the most recent OS and application security patches must be installed and updated with the most current version;
    - Access to the information must be restricted by requiring a unique user account ID and strong password for each user who will access the information or use the computer on which it sits;
    - Computer accounts must not be shared.
    - A password protected screen saver set to 15 minutes or less must be enabled; and,
- All computers used to store and/or process PROTECTED information, which are also connected to the Internet, should reside behind a network router that is securely-configured using industry best practices (e.g. NAT-enabled firewall, password-protected and documented configuration, security logging enabled, maintained and reviewed, filtered access).
- Security event logging must be enabled and logs kept for a minimum of 90 days.
- If there is a requirement to service a computer that is used to store and/or process PROTECTED information outside of the Contractor's premises, any hard disk(s) containing PROTECTED information must be removed and secured with the Contractor prior to the computer being removed from the premises.
- If it has been determined that a computer hard disk used to store and/or process PROTECTED information is no longer serviceable, the hard disk must be surrendered to the Project Authority for destruction.

- When devices such as a computer hard drives, portable hard drives, USB storage drives and any other devices used to store/process PROTECTED information are no longer required to store/process the infomlation, the information must be securely deleted and the remaining free space on the device securely wiped, in accordance with industry best practices
- When PROTECTED information is being displayed on a computer screen or being viewed in printed format, it must not be viewable by unauthori zed persons.
- If remote access to the contractor's Information System (i.e. computers & storage devices) and the PROTECTED information contained therein is required, the remote access configuration must be securely-configured using industry best practices (e.g. enc1ypted connection, two-factor authentication, security logging, no split tunneling, access control lists, remote access software provided by Contractor to employee).
    - Any employees using the remote access must also meet all requirements listed in this document with regards to their remote location and equipment used there.