

Annex A

SRCL

Security Guide

Processing of Sensitive Information

Public Works and Government

Services Canada

(PWGSC)

Table of Contents

1. INTRODUCTION.....	3
2. MANDATORY PREREQUISITES	3
2.1 PWGSC VALIDATION FOR PHYSICAL SECURITY	3
2.2 PERSONNEL SECURITY	3
2.3 INFORMATION SECURITY	4
2.4 SECURITY POLICY COMPLIANCE MONITORING	4
3. MINIMUM IT SECURITY REQUIREMENTS.....	4
3.1 IT SECURITY POLICY COMPLIANCE AND MONITORING	4
3.2 ADHERENCE TO GOVERNMENT OF CANADA POLICIES	5
3.2.1 Prevention.....	5
3.2.2 Detection.....	7
3.2.3 Response and Recovery	7
4. IT SYSTEM CONNECTIVITY	8

1. Introduction

This document outlines the IT Security requirements for the Department's current contract # EP008-112560 with the Contractor for the processing of sensitive data up to and including the level of Secret. 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 in order that the processing of sensitive information be approved by the Department's IT Security Coordinator (ITSC).

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 are based on the mandatory requirement that the physical premises have been inspected, certified and accredited to process and store sensitive information by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services. The Departmental Security Officer's (DSO) office will validate the certification and notify the ITSC.

A CISD Field Industrial Security Officer (FISO) will perform a bi-annual inspection to ensure that premises PWGSC certification is maintained.

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 Public Works and Government Services Canada sensitive information must attend a training/briefing session coordinated and delivered by the Public Works and Government Services Canada DSO and ITSC.

2.3 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 Public Works and Government Services Canada. 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 must adhere to RCMP G1-009 "Transport and Transmittal of Protected and Classified Information". Public Works and Government Services Canada personnel may only transport documents associated with a Public Works and Government Services Canada contract into or out of the security zone with the approval of the Public Works and Government Services Canada DSO.

2.4 Security Policy Compliance Monitoring

On a frequency to be determined by the Safety, Security and Emergency Management Division (SSEMD), Public Works and Government Services Canada retains the right to conduct inspections of the Contractor's facilities to ensure compliance with Government of Canada standards and policies with respect to the handling, storage and processing of sensitive information.

3. Minimum IT Security Requirements

3.1 IT Security Policy Compliance and Monitoring

On a frequency to be determined by Technology Services Division/Information Technology Security, Public Works and Government Services Canada retains the right to conduct inspections of the Contractor's facilities to ensure compliance with Government of Canada standards and policies with respect to prevention, detection, response and recovery requirements in the Operational Security Standard: Management of Information Technology Security.

3.2 Adherence to Government of Canada Policies

All information technology related operations must adhere to the overall requirements outlined in Treasury Board's Operational Security Standard: Management of Information Technology Security. Specifically, sections 16-18 referring to prevention, detection, response and recovery.

3.2.1 Prevention

Prevention safeguards protect the confidentiality, integrity, and availability of information and IT assets.

3.2.1.1 Physical Security within the IT Security Environment

The Contractor will provide the Public Works and Government Services Canada ITSC with the list of physical safeguards which are implemented in the facility which is used to process and store sensitive information. All equipment processing sensitive information is to reside in a security zone.

The equipment within the security zone, which is used to process the sensitive information, must be either standalone or on an island network which is self-contained, used for the purposes of processing the information related to the contract and have no external connection to the internet or other network, internal or otherwise.

The island network must only be used for the processing and storage of information related to contracts with Public Works and Government Services Canada and no other party.

The use of wireless technology for the processing of sensitive information is prohibited.

3.2.1.2 Storage, Disposal and Destruction of IT Media

All material such as CD/DVDs, flash/thumb drives, workstation hard disks, server hard disks, backup tapes and any other devices used to process or store sensitive information must be identified and itemized by model and serial number for hard disks, and by label for any other media which cannot be identified by model or serial number. These devices or material must be retained and properly stored or disposed of by Public Works and Government Services Canada IT Security personnel in the event of failure and replacement of the equipment or termination of the final contract.

The Public Works and Government Services Canada ITSC must be provided with the list of equipment and media being used. In addition, only equipment and media that has been identified, itemized and documented may be used to process sensitive information associated with Public Works and Government Services Canada contracts.

In the event that equipment requires maintenance, support or replacement, no hardware associated with the processing or storage of sensitive information may be given to an outside vendor.

All media, when not in use, must be stored in a storage container which is RCMP-approved for the storage of sensitive information to the level of Protected B (G1-001 "Security Equipment Guide". The storage container must be verified by CISC and validated by Public Works and Government Services Canada DSO's Office.

3.2.1.3 Authorization and Access Control

The Contractor must provide the Public Works and Government Services Canada ITSC with a list of all individuals who have access to the sensitive information being processed for the Department, along with the Contractor's 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, the Contractor must provide only the minimum access required for individuals to perform their duties.

3.2.1.4 Mobile Computing and Teleworking

Due to the fact that the requirements have stipulated an island-network configuration, mobile computing and teleworking need not be expressly addressed; however, it is important to state that the processing of sensitive information associated with Public Works and Government Services Canada related contracts may only be performed in facilities which have been validated by the Public Works and Government Services Canada DSO.

3.2.1.5 Emanations Security

The Operational Security Standard: Management of Information Technology Security states that organizations should use TEMPEST protection for Top Secret and Protected C information, when justified by a Threat and Risk Assessment. A TRA should be performed in order to ascertain whether or not TEMPEST protection is appropriate.

3.2.1.6 Telecommunications Cabling

In the event an island network is used rather than standalone equipment, it is important to control and monitor access to telecommunications wiring, spaces and pathways to avoid inadvertent or deliberate connection to any other network.

3.2.1.7 Software Integrity and Security Configuration

The Contractor should configure the security their operating systems and application software being used to process sensitive information in accordance with security best practices (such as the Microsoft Security Compliance Toolkits for servers and clients documentation). The Contractor must implement safeguards to "harden" servers and workstations processing sensitive information, and detail that information in a document to be delivered to the Public Works and Government Services Canada ITSC.

3.2.1.8 Malicious Code

Due to the isolation of the systems being used to process sensitive information, standalone or island network, these systems are less exposed to malicious code such as viruses, Trojan horses, and network worms; however, without proper procedures for introducing new equipment or information into the environment, they are still vulnerable. Therefore, the Contractor must install, use and regularly update antivirus software and conduct scans on all electronic files from external systems.

3.2.2 Detection

It is important to have the ability to detect security related issues within the operating environment which processes sensitive information. Even though the systems are isolated, it is still useful to use sources such as system logs, event viewer, virus protection software and other system tools to monitor systems. In order to adequately protect information there must exist the ability to detect activity such as unauthorized access, unplanned disruption of systems or services or unauthorized changes to system hardware, firmware, or software. Detection mechanisms which are used by the Contractor must be documented and provided to the Public Works and Government Services Canada ITSC.

3.2.3 Response and Recovery

3.2.3.1 Incident Response

Public Works and Government Services Canada requires the Contractor to have a documented incident response process. All documentation pertaining to incident response must be provided to the Public Works and Government Services Canada ITSC.

3.2.3.2 Incident Reporting

It is paramount that the Public Works and Government Services Canada DSO and ITSC are made aware of any security-related incidents with respect to the facilities and equipment used to process and store sensitive information associated with Public Works and Government Services Canada contracts.

The Contractor must report any security-related incidents to the Public Works and Government Services Canada DSO and ITSC within two hours of an incident being detected or reported.

3.2.3.3 Recovery

The ability to recover systems and information is extremely important in any IT environment. Public Works and Government Services Canada requires the Contractor to demonstrate the ability to address systems recovery by providing documentation relating to systems and server backup policies (e.g. processes used, tests restores, retention periods and storage of backup media). This documentation shall be forwarded to the Public Works and Government Services Canada ITSC.

4. IT System Requirements

The contractor is required to meet the following criteria, provide the required Information System (IS) topology and identified security documentation of their systems to the PWGSC Project Information System Security Officer (ISSO), and to the Industrial Security Operations Division (ISOD) at PWGSC.

4.1 Contractor IT System Requirements

- 4.1.1 Identify the following individuals for the contractor Information Technology Systems (IT Systems):
- 1 Information Technology System Manager, and
 - 2 Information Technology System Security Officer
- 4.1.2 Describe the architecture of the contractor's IT Systems that are to connect/communicate to the PWGSC IT Systems.
- 4.1.3 Provide a Topology, Block level Diagram, of the contractor's IT Systems. The drawing is to indicate the interface devices (ACM, firewalls, modems Network security {A/B} Switches, etc)
- 4.1.4 Provide detail regarding any modems attached to the contractor's IT Systems including identifying to what other IT Systems the modem connects.
- 4.1.5 Any IT Systems connected to PWGSC IT Systems must be dedicated to PWGSC use only. No external connections to other contractor IT Systems or public domains is permitted without express consent of PWGSC's ITSC.
- 4.1.6 PWGSC is to be provided with results of IT Systems Security Inspections, vulnerability assessment and penetration test on the contractor's IT Systems connected to or schedule for connection to PWGSC IT Systems.
- 4.1.7 Any Certification or Accreditation documentation on the contractor's IT Systems is to be provided to PWGSC prior to connection to the PWGSC IT Systems.
- 4.1.8 Access to the contractor IT Systems connected to the PWGSC IT Systems for this contract is limited to personnel with the appropriate security clearance and who have a valid "need-to-know".
- 4.1.9 Unique LOGIN ID/passwords are to be used by all contractor personnel accessing either the contractor or PWGSC IT Systems.
- 4.1.10 Audit logs of the contractor's and PWGSC IT Systems are maintained and reviewed on a regular basis by PWGSC personnel.
- 4.1.11 Ensure all media is marked at the appropriate security level and is secured accordingly to PWGSC standards.

- 4.1.12 Utilize a Configuration Management Plan that tracks changes to the contractor's IT Systems.
- 4.1.13 Identify Contractors IT Systems patch management procedures.
- 4.1.14 Changes to the connecting Contractor's IT Systems require prior approval of PWGSC.
- 4.1.15 The contractor's IT Systems must be available at all times for PWGSC security inspection and verification.
- 4.1.16 Contractor will not conduct Penetration Test, Vulnerability scans, port scans or any other intrusive attack against the PWGSC IT Systems.