RDIMS #2188404

J85
Propulsion Group Sustainment
(PGS)

Annex G

PROCESSING OF SENSITIVE INFORMATION - IT SECURITY REQUIREMENTS

DEPARTMENT OF NATIONAL DEFENCE / CONTRACTOR NAME

Annex G – IT Security Requirements

1. INTRODUCTION

This document outlines the IT Security requirements for the Department's/Contractor current contract # (to be identified) with *(company name)* for the processing of sensitive data up to and including the level of Protected A. 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 DAEPM(FT) Security Manager (Sec Mgr) / Information System Security Officer (ISSO).

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. PSPC 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 Services and Procurement Canada (PSPC). The Departmental Security Officer's (DSO) office will validate the certification and notify the Sec Mgr / ISSO.

A CISD Field Industrial Security Officer (FISO) will perform a bi-annual inspection to ensure that premises PSPC 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 *(company name)* personnel handling Department of National Defence (DND) Government of Canada sensitive information must attend a training/briefing session coordinated and delivered by the DND DSO, Sec Mgr / ISSO.

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 DND. 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*". (*Company name*) personnel may only transport documents associated with a DND contract into or out of the *security zone* with the approval of the DND's DSO.

2.4. Security Policy Compliance Monitoring

On a frequency to be determined by the Safety, Security and Emergency Management Division (SSEMD), DND retains the right to conduct inspections of the (*company name*) facility 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, DND retains the right to conduct inspections of the (company name, at location - if known) facility 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 the *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.

3.2.2 Physical Security within the IT Security Environment

(Company name) will provide the Sec Mgr / ISSO 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* as per RCMP - *Guide to the Application of Physical Security Zones*" (G1-026).

The equipment within the *security zone,* which is used to process the sensitive information, must be either standalone or on an '*island*' network (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) or is authorized on the (*company name*)'s Corporate Network).

This island network must only be used for the processing and storage of information related to contracts/subcontracts with DND and no other party.

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

3.2.3 Cryptography, Network Security and Perimeter Defence

The electronic storage of Protected A and/or Protected B information associated with this contract must be within a CISD approved IT environment.

Electronic transmission of Protected A information should be encrypted when supported by a Threat and Risk Assessment. However, Protected B information must be encrypted.

For Protected B information, the (*company name*) must segregate its networks into IT security zones and implement perimeter defence and network security safeguards. CSEC provides the ITSG-38 and ITSG-22 guidelines on this specific subject. As well, the Contractor/Supplier must apply strict control of all access to the protected zone where the information associated with this contract resides. Network perimeter defence safeguards (e.g. firewalls, routers) must be used to mediate all traffic and to protect servers that are accessible from the internet. The (*company name*) must use CSEC approved encryption technology to ensure confidentiality, integrity, authentication and non-repudiation.

The Need-to-Know principle must always be applied for Protected A and Protected B information and transmission must be restricted only to CISD approved recipients.

3.2.4 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 DND IT Security personnel in the event of failure and replacement of the equipment or termination of the final contract.

The Sec Mgr / ISSO 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 DND 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 Secret (G1-001 "*Security Equipment Guide*". The storage container must be verified by CISD and validated by the DND DSO's Office.

3.2.4.1 Authorization and Access Control

(Company name) must provide the Sec Mgr / ISSO with a list of all individuals who have access to the sensitive information being processed for the Department, along with (company name) 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', (company name) must provide only the minimum access required for individuals to perform their duties.

3.2.4.2 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 DND-related contracts/subcontracts *may only* be performed in the facility which has been validated by the DND DSO.

3.2.4.3 Telecommunications Cabling

In the event a Local Area Network or the Corporate 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.

3.2.4.4 Software Integrity and Security Configuration

(company name) 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), Directorate of Aerospace Equipment Program Management (DAEPM) documentation. DAEPM must implement safeguards to "harden" servers and workstations processing sensitive information, and detail that information in a document to be delivered to the Sec Mgr / ISSO.

3.2.4.5 Malicious Code

(company name) must install, use and regularly update antivirus software and conduct scans on all electronic files from external systems.

3.2.5 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 (company name) must be documented and provided to the Sec Mgr / ISSO.

3.2.6 Response and Recovery

3.2.6.1 Incident Response

The Policy on Government Security requires departments to ‘establish mechanisms to respond effectively to IT incidents and exchange incident-related information with designated lead departments in a timely fashion’. Similarly, DND requires (company name) to have a documented incident response process. All documentation pertaining to incident response must be provided to the Sec Mgr / ISSO.

3.2.6.2 Incident Reporting

It is paramount that the DND DSO and Sec Mgr / ISSO are made aware of any security-related incidents with respect to the facilities and equipment used to process and store sensitive information associated with DND contracts and subcontracts if applicable.

(Company name) must report any security-related incidents to the DND DSO and Sec Mgr / ISSO within *two hours* of an incident being detected or reported. CISD shall also be notified of such incident.

3.2.6.3 Recovery

The ability to recover systems and information is extremely important in any IT environment. The Department of National Defence requires that (company name) 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 Sec Mgr / ISSO.