Annex "D"

IT Security Controls

Introduction

This document outlines the IT Security requirements for the MPCC contract #MPCC- -
for the processing of sensitive data up to and including the level of Protected B. In accordance with the 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 MPCC's Departmental Security Officer (DSO); Bruno Prévost, Tel: 343.543-2609, Email: bruno.prevost@mpcc-cppm.gc.ca.

Security is based upon layers of protection; that is, in order for the requirements of the IT Security (ITS) to effectively safeguard the information, 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.

1. Mandatory Prerequisites

1.1 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 (PWGSC). The Departmental Security Officer's (DSO) office will validate the certification and notify the IT Specialist.

1.2 Security Policy Compliance Monitoring

The DSO's office will request a copy of the IT Security Inspection report, recommendations and vendor responses.

The MPCC has the option to request the contractor to attend a Security/IT Security briefing session. In addition, on a frequency to be determined by the Safety, Security and Emergency Management Division (SSEMD), the MPCC 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 protected/classified information.

2. Minimum IT Security Requirements

2.1 IT Security Policy Compliance and Monitoring

On a frequency to be determined by Technology Services Division/Information Technology Security, the MPCC retains the right to conduct inspections of the 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.

2.2 Storage, Disposal and Destruction of IT Media

All material such as CD/DVDs, flash/thumb drives, workstation hard disks, server hard disks and any other devices used to process or store protected information (including photocopiers, scanners and

printers) must be retained and properly wiped or sanitized in a manner adhering to CSEC ITSG-06: Clearing And Declassifying Electronic Data Storage Devices upon termination of the final contract.

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

2.3 Mobile Computing and working remotely

Safeguard all electronic information on MPCC's servers by using an issued laptop with PKI access on the server as per MPCC internal procedures for information up to and including Protected B. For any documents classified as Secret, access will only be provided on site at MPCC offices and shall not be stored on the MPCC server.

Store the laptop (Protected B) in a container appropriate for the information (i.e. a locked cabinet) as per MPCC security policy.

2.4 Incident Reporting

It is paramount that the MPCC and IT Specialist are made aware of any security-related incidents with respect to the facilities and equipment used to process and store sensitive information associated with MPCC contracts.

The contractor must report any security-related incidents to the DSO and IT Specialist as soon as possible of an incident being detected or reported.