[redacted]

51019-14-6001

Processing of Protected Information

Contract Security Requirements

IT Security

Veterans Affairs Canada.

1. INTRODUCTION **3**

2. MANDATORY PREREQUISITES **3**

2.1 INFORMATION SECURITY 3

3.MINIMUM IT SECURITY REQUIREMENTS **3**

3.1. IT SECURITY POLICY COMPLIANCE AND MONITORING 3

3.2. ADHERENCE TO GOVERNMENT OF CANADA POLICIES 3

3.2.1.Prevention *4*

3.2.1.1.Physical Security within the IT Security Environment 4

3.2.1.2.Storage, Disposal and Destruction of IT Media 4

3.2.1.3.Authorization and Access Control 5

3.2.1.4.Mobile Computing and Teleworking 5

3.2.1.5.Emanations Security 5

3.2.1.6.Telecommunications Cabling 5

3.2.1.7.Software Integrity and Security Configuration 5

3.2.1.8.Malicious Code 5

3.2.2.Detection *6*

Response and Recovery *6*

3.2.2.1.Incident Response 6

3.2.2.2.Incident Reporting 6

3.2.2.3.Recovery 6

3.2.2.4 Work Location 6

1. Introduction

This document outlines the IT Security requirements for the Department's current contract 51019-14-6001 for the processing of protected data up to and including Protected A. In the 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 protected information be approved by the Department's IT Security Coordinator (ITSC).

2. Mandatory Prerequisites

2.1 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 Veterans Affairs Canada. Any covering letter, transmittal form or circulation slip will be marked to indicate the highest level of classification of the attachments.

Personnel may only transport documents associated with a Veterans Affairs Canada contract into or out of the operational zones with the approval of the Veterans Affairs Canada DSO.

3.0 Minimum IT Security Requirements

3.1 IT Security Policy Compliance and Monitoring

On a frequency to be determined by the Information Technology (IT) Services section, Veterans Affairs Canada retains the right to conduct inspections of the contractor's facility to ensure compliance with Government of Canada standards and policies with respect to prevention, detection, response and recovery requirements as prescribed 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.

3.2.1.1 Physical Security within the IT Security Environment

The contractor will, as requested by the Veterans Affairs Canada ITSC, provide a list of physical safeguards which are implemented in the facility which is used to process and store protected information. All equipment processing protected information is to reside in a operations zone.

The equipment within the operations zone, which is used to process the protected 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).

The *island* network must only be used for the processing and storage of information related to contracts with the Veterans Affairs Canada and no other party.

The use of wireless technology for the processing of protected information is prohibited without the express written approval of the VAC DSO.

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 protected 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 Veterans Affairs Canada IT Security personnel in the event of failure and replacement of the equipment or termination of the final contract.

When requested, the Veterans Affairs 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 protected information associated with the Veterans Affairs Canada contract.

In the event that equipment requires maintenance, support or replacement, no hardware associated with the processing or storage of protected information may be given to an outside vendor without the approval of the ITSC.

All media, when not in use, must be stored in a storage container which is approved for the storage of information up to and including the Protected A level.

3.2.1.3 Authorization and Access Control

Within two weeks of contract award the contractor must provide the Veterans Affairs Canada ITSC with a list of all individuals who have access to the protected information being processed for the Department, along with the contractor's 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 protected information associated with Veterans Affairs Canada related contracts *may only* be performed in the facility which has been validated by the Veterans Affairs Canada DSO.

3.2.1.5 Emanations Security

The highest level of information processed under this contract is Protected A, as such, there are no TEMPEST protection requirements at this time.

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 protected information in accordance with security best practices (such as the Microsoft Security Compliance Toolkits for servers and clients, Veterans Affairs Canada documentation. The contractor must implement safeguards to "harden" servers and workstations processing protected information, and detail that information in a document to be delivered to the Veterans Affairs Canada ITSC.

3.2.1.8 Malicious Code

Due to the isolation of the systems being used to process protected 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 protected 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 Veterans Affairs Canada ITSC upon request.

Response and Recovery

3.2.2.1 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, Veterans Affairs Canada requires the contractor to have a documented incident response process. All documentation pertaining to incident response must be provided to the Veterans Affairs Canada ITSC upon request.

3.2.2.2 Incident Reporting

It is paramount that Veterans Affairs Canada's DSO and ITSC are made aware of any security-related incidents with respect to the facilities and equipment used to process and store protected information associated with Veterans Affairs Canada contracts.

The contractor must report any security-related incidents to the Veterans Affairs Canada DSO and ITSC within *two hours* of an incident being detected or reported.

3.2.2.3 Recovery

The ability to recover systems and information is extremely important in any IT environment. Veterans Affairs 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 Veterans Affairs Canada ITSC, upon request.

3.2.2.4 Work Location

All data input, processing, storage, accessing, and electronic back-ups are to be domestically processed and stored in Canada.