Department of National Defence (DND)

Information Technology Security Requirements

For

Contract W8482-168150

RELEASE HISTORY

Serial	Date Release	Version	Amendments Details
1	17 Apr 2018	1	Initial Draft
1	20 Apr 2018	1.1	Added MFD maintenance / disposal (3.8.4)
1	25 Apr 2018	1.2	Added rules on: IT Connections (2.5.7) Topology diagram (3.3.3) Log files modify / delete (3.3.9)
1	26 Apr 2018	1.3	Added advice on IT Security requirements selection (1.3)
1	03 May 2018	1.4	Amended as per comments from Mr. Lamoureux

1. INTRODUCTION

1.1 This document outlines the Information Technology (IT) Security requirements for the Department of National Defence's (DND) current contract W8482-168150 for the processing, production and/or storage of sensitive information up to and including the level of SECRET. Considering the IT portion of the Security clearance being contract specific, the intent of this document is to establish the minimum IT Security safeguards required for the processing, production and/or storage of sensitive information be approved by the DND authority.

1.2 Security is based upon layers of protection; that is, in order for the requirements of the IT Security (ITSEC) to effectively safeguard the information, they must be preceded and supported by other aspects of security and their associated policies. Prior to engaging in the contracted efforts, in accordance with the Policy on Government Security (PGS) and ITSEC related Policy, Directive and Standards, physical, personnel, procedural and information security safeguards, must exist prior to the implementation of ITSEC safeguards.

1.3 As a part of selecting contractual IT Security safeguards, Project Leads should carefully consider the impact of the selected IT security safeguards on cost, schedule and operational requirements. Project Leads should be looking for a reasonable trade-off between the incremental cost of security requirements and the risk mitigation that would result from their use. The DND DIM Secur can assist Project Leads with these decisions, when requested.

2. MANDATORY PREREQUISITES

2.1. PSPC Validation for Physical Security

2.1.1 The application of the ITSEC safeguards listed in this document are based on the *mandatory requirement* that the physical premises have been inspected, assessed and authorized to process, produce and store SECRET information. Validation must be provided by the Canadian Industrial Security Directorate (CISD), Public Services & Procurement Canada (PSPC).

2.1.2 The Contractor must inform CISD and the DND Project Lead of all physical sites where contractual information will be processed, produced and/or stored. This includes as applicable but is not limited to the main/secondary Contractor's offices, construction site, back-up storage location, and partner's / Sub-Contractor's offices.

2.1.3 Upon validation, CISD will notify the DND Project Lead, the Director Defence Security Operations (DDSO) Industrial Security Lead and the Directorate Information Management Security (DIM Secur) Operations of the successful completion of this requirement. Every site must be granted a Facility Security Clearance (FSC) and a Document Safeguarding Capability (DSC) and be cleared for SECRET IT Security by CISD prior to be authorized to process, produce and/or store government sensitive information, up to and including SECRET.

2.1.4 IT Links (when applicable) must also be validated by CISD before it can be used to transfer any contractual SECRET information.

2.2. Physical Security

2.2.1 The IS (identified herein as the W8482-168150 IS) must be installed and be operated in a security zone or in a temporary security zone in accordance with the RCMP G1-026.

2.2.2 Processing, production and/or storage of contractual information must only be performed in the facility(s) which has been authorized by CISD.

2.2.3 Processing, production and/or storage of contractual information must not be performed outside Canada.

2.2.5 Mobile computing / Teleworking involving the W8482-168150 IS is not authorised on this contract.

2.3. Personnel Security

2.3.1 All Contractor personnel who have access to processed, produced or stored contractual SECRET information must each hold a valid personnel security clearance at the SECRET level,

and have a "*need to know*". Contractor's SECRET security clearance must be granted and be tracked by CISD.

2.3.2 All Contractor personnel handling contractual sensitive information must be provided training/briefing session coordinated and delivered by the Company Security Officer (CSO or by the Alternate CSO (ACSO). This training must make reference to the Industrial Security Manual (ISM) and other security publications as determined by the DND Project Lead.

2.3.3 No foreign national can have the capability to affect the Confidentiality, Integrity and Availability of the data without a valid personnel security clearance at the SECRET level and the prior approval from the CISD International section and the DND Project Lead.

2.3.4 Access to the zone where contractual information is being processed, produced and/or stored is prohibited to visitors, personnel not holding a valid personnel security clearance at the SECRET level and personnel not previously authorised unless escorted at all times by an authorised Contractor.

2.4. Procedural Security

2.4.1 The Contractor must create System IT Security Orders and Standard Operating Procedures (SOP) specifying as a minimum; roles and responsibilities, access management, acceptable use and incident management as it relates to the operation and maintenance of W8482-168150 IS.

2.4.2 All personnel having access to the IS must read the System IT Security Orders and sign a user agreement form.

2.4.3 The W8482-168150 IS must be administered and be maintained internally by individual(s) possessing at least, valid personnel security clearance at the SECRET level. The W8482-168150 IS must not be remotely accessible.

2.4.4 The Contractor must continually monitor its overall security posture including; physical, personnel, procedural, information and IT security and inform CISD and the DND Project Lead of any changes that could potentially impact the security of the contractual information.

2.5. Information Security

2.5.1 Contractual information must be exchanged between the DND Project Lead, and all levels of Contractor/Sub-Contractor companies using hard copy documents, IT media and/or an approved IT link. Hard copy documents and IT media must be handled and be transported in accordance with Government of Canada guidelines (RCMP G1-009 "Operational Security Standard on Physical; Security").

2.5.2 All hard copy documents and other media must be marked with the appropriate security designation or classification and be afforded a unique identifier to ensure positive control and tracking.

2.5.3 All hard copy documents and IT media will be packaged appropriately and be transmitted with a covering letter and a transmittal form or circulation slip marked to indicate the highest level of designation or classification of the attachments as stated in the contracts Security Requirements Check List (SRCL) as well as the date of transmission, the document unique identifier, the originator, and the destination.

2.5.4 All contractual information must be segregated from other contractual and corporate information in a way which allows all contractual information to be immediately security wiped upon request from CISD or the DND Project Lead.

2.5.5 Contractual information must not be stored using external "cloud" technology.

2.5.6 IT links are not authorized between the DND environment and the Contractor or the Contractor and any other level of Contractor/Sub-Contractor unless CISD and the DND Project Lead have been made aware and have authorised it. The IT link (if applicable) must be inspected and be validated by CISD.

2.5.7 IT Connections are not authorized between the W8482-168150 IS and any other network, system or equipment unless CISD and the DND Project Lead have been made aware and have authorised it. An additional IT security inspection may be required to validate and authorize the IT connection.

2.5.8 Encryption is normally used to protect information at rest (residing on local system) or during transport. In the case of this contract, encryption will not be necessary due to the use of removable hard drives (see para 3.3.5), the requirement to lock all IT media when not being used (see para 3.5.5) and the absence of any IT Link (see para 2.5.6) preventing the transmission of sensitive information.

3. MINIMUM IT SECURITY REQUIREMENTS

3.1. IT Security Policy Compliance and Monitoring

3.1.1 On a frequency and schedule to be determined by the DND Information Technology Security Coordinator (ITSC), DND retains the right to conduct inspections of the Contractor's facility to ensure compliance with the IT Security Requirements herein as well as the Government of Canada standards and policies with respect to the prevention, detection, response and recovery requirements as depicted in the TBS *Operational Security Standard: Management of Information Technology Security* (MITS).

3.2. IT Equipment

3.2.1 A list of all equipment forming the W8482-168150 IS must be maintained by the Contractor. The list of equipment must contain but not be limited to: equipment description, quantity, make and model. If requested, the list of equipment must be made available to CISD and the DND Project Lead.

3.2.2 The Contractor must inform CISD and the DND Project Lead of any major change to the W8482-168150 IS IT equipment.

3.3. IT System Configuration

3.3.1 The equipment used to process, produce and/or store the contractual information must consist of TEMPEST equipment and must be labelled commensurate with the contractual information sensitivity SECRET level.

3.3.2 The W8482-168150 IS must be configured as a Closed Local Area Network with no external connection.

3.3.3 A topology diagram of the W8482-168150 IS must be provided upon request, to CISD and the DND Project Lead. The diagram must consist of a high level system design and include if applicable any IT links to other entities and/or connections to other networks / systems.

3.3.4 All equipment interconnectivity must be using fibre optic cables and must be identifiable from the corporate system wiring, must be controlled and monitored to prevent inadvertent or deliberate connection to any unauthorised equipment, network or infrastructure and, must be run in separate conduits.

3.3.5 Workstation(s) and server(s), must be configured with removable hard drives.

3.3.6 The W8482-168150 IS must operate on a supported Operating System (OS). OS security patches must be updated regularly; at least on a monthly basis. The OS must be

configured to disable unnecessary processes and ports. The W8482-168150 IS SOP must identify the frequency and the method used to update the OS security patches and provide details on the OS configuration.

3.3.7 A supported antivirus application must be installed and be operational on the W8482-168150 IS. The antivirus definition files must be updated regularly; at least on a monthly basis. The antivirus application must be configured to automatically scan the W8482-168150 IS at power-on or on a set interval. Every new file introduced onto the W8482-168150 IS must be scanned for viruses. The W8482-168150 IS SOP must identify the frequency and the method used to update its definition files as well as the configuration of the antivirus application.

3.3.8 Only applications required by the contract must be installed on the W8482-168150 IS. Application patches must be kept up to date and be managed through a defined configuration management process. The W8482-168150 IS SOP must list every installed application and identify the application patch management process.

3.3.9 OS log files must be active and be reviewed at least on a monthly basis. The review must consist of but not be limited to: unsuccessful login attempts, unauthorised changes to the system hardware / firmware / software, unusual system behaviour, unplanned disruption of systems / services, system errors, etc. Only system administrators shall be allowed to modify or delete log files. The W8482-168150 IS SOP must identify the frequency and the method used to review OS log files.

3.3.10 The use of wireless capabilities on the W8482-168150 IS is strictly prohibited.

3.4. Authorization and Access Control

3.4.1 The Contractor must provide the DND Project Lead with a list of all individuals who have access to the contractual information. The list must also provide the type of account set for each user.

3.4.2 Specific user account must be created for each user. User accounts must never be share.

3.4.3 Specific administrator account must be created for each system administrator. If an administrator is also required to operate the W8482-168150 IS, a separate user account must be created for his/her operation of the system.

3.4.4 There must be no generic account on the W8482-168150 IS.

3.4.5 User accounts must be configured for limited privileges and must allow access only to files and folder required by the users to perform their duties.

3.4.5 Every account must be protected by a password. The passwords must: never be shared, consist of at least 8 characters and be composed of a combination of a minimum of three of the following: upper case, lower case, numerical and special character. Passwords must be changed at first login and subsequently, every 90 days. The OS remember option must be disabled, and the last 10 password changes be remembered.

3.4.7 System default administrator passwords must be changed. The new administrator password must be written and be placed in a sealed envelope. The envelope must be safeguarded commensurate with the highest level of contractual information SECRET and be locked in an approved container RCMP secure cabinet.

3.4.8 The W8482-168150 IS SOP must include an Authorization and Access Control process depicting the user addition and removal process.

3.5. IT Media

3.5.1 Every IT media, including removable and external hard drives, used to process, produce and/or store contractual information must be dedicated to this contract only.

3.5.2 Every IT media, including removable and external hard drives, must be afforded a unique identifier to ensure positive control and tracking.

3.5.3 Every IT media, including removable and external hard drives, must be identified and itemized by Designation or Classification, releasability caveat, model and serial number (if applicable). A list of all IT media, including removable and external hard drives, must be maintained by the Contractor. The list of IT media must contain but not be limited to: media description (CD/DVD, Memory stick ...), serial number if applicable, and unique identifier. If requested, the list of IT media must be made available to CISD and the DND Project Lead.

3.5.4 Every IT media, including removable and external hard drives, must be labelled. The label must contain: the highest level of information sensitivity SECRET it contains, the Contract number and the IT media unique number. If a label cannot be affixed directly on the IT media (i.e. memory sticks), the label must be attached to it using a string or other means.

3.5.5 All IT media, including removable and external hard drives, must be safeguarded commensurate with the contractual information sensitivity level. When not being used, all IT media (including failed, life cycled and longer required media) must be locked in an approved container RCMP secure cabinet.

3.5.6 The location of all IT media must be controlled via the use of a log book. The “IT media log book” must contain but not be limited to: the media description, unique identifier, the date it was removed from and returned to the approved container and, the initials of the individual who took the media.

3.5.7 In the event that equipment requires maintenance, support or replacement, NO IT MEDIA containing contractual information must be given or be made available to an outside vendor or service provider.

3.5.8 Throughout the duration of the contract, IT media that failed, is being life cycled or is no longer required must be disposed of in accordance with the "Disposal" section of this document.

3.6. Document Printing / Reproduction

3.6.1 The Contractor is authorized to print and/or reproduce contractual sensitive documents within the Contractor's premises. External printing / reproduction services must be approved / authorized by CISD and the DND Project Lead.

3.6.2 Printers, plotters, scanners and/or Multi-Function Devices (MFD) used on W8482-168150 must not be equipped with internal hard drives. If unfeasible, printers, plotters, scanners and/or MFD must be equipped with removable hard drives.

3.6.3 The use of MFD is authorized if connected only to the W8482-168150 IS. Connection to other devices, network or telephone line is strictly prohibited.

3.6.4 When controlled documents (as identified by the DND Project Lead) are being reproduced, every copy of the original document must be afforded a unique identifier to ensure positive control and tracking.

3.6.5 In the event that printing and reproduction services are sub-contracted, the Sub-Contractor must abide by the contract specific "**Information Technology Security Requirements**" herein.

3.6.6 For the maintenance and disposal of printers, plotters, scanners and/or MFD, instructions provided in the "Disposal" section herein must be applied.

3.7. Recovery

3.7.1 The contractual information must be backed-up regularly (at least once a week) and be safeguarded at a remote location. If the Contractor does not have a remote location to safeguard the backups, arrangements can be made with the DND Project Lead. If backups are safeguarded with another contractor, CISD and the DND Project Lead must be informed, validate and authorise the initiative. The W8482-168150 IS SOP must include details on the back-up frequency, methodology and storage.

3.7.2 The Contractor must elaborate and document a system disaster recovery plan. The W8482-168150 IS SOP must include details on the recovery, restoration, tests frequency, and methodology.

3.8. Disposal

3.8.1 The disposal of IT media (media that failed, is being life cycled or is no longer required), including removable and external hard drives, used on W8482-168150 must be authorized in advance by the DND Project Lead and must be documented / tracked. The local disposal of IT media is prohibited.

3.8.2 The disposal of IT media must be tracked via the use of a certificate of destruction (DND Project Lead will provide template) and a document Transit and receipt form (DND Project Lead will provide template). The Contractor must retain a copy of every IT disposal evidence document and if requested, must made the evidence available to CISD and the DND Project Lead.

3.8.3 All IT media containing contractual information must be given to the DND Project Lead at the end of the contract.

3.8.4 The following process must be applied prior to removing printers, plotters, scanners and/or Multi-Function Devices (MFD) used on W8482-168150 for maintenance or disposal:

3.8.4.1 If the equipment contains an internal/external hard drive or any other non-volatile memory device, the hard drive and/or non-volatile memory must be removed and be disposed of as indicated above.

3.8.4.2 Volatile Memory (RAM, DRAM, SRAM) must be sanitized by removing all power for 24 hours. Ensure there is no internal power to the memory (e.g. internal batteries).
NOTE: If there is doubt concerning the removal of all internal power to Volatile Memory in highly sensitive equipment that is being decommissioned, consider removing the Volatile Memory (RAM, DRAM, SRAM).

3.8.4.3 Any stickers or security markings on the device must be removed.

3.8.4.4 For MFDs used to process classified information, at least 50 pages of unclassified material (not blank) must be photocopied in order to remove any possible data on the drums or belts when so equipped.