Annex "E"

IT Security Requirements Technical Document

IT Security, Correctional Service Canada

Contract: 21201-16-2168247
Date: 12 January 2015

The following are the IT Security Requirements for the above mentioned contract. They are derived from the Operational Security Standard: Management of Information Technology Security (MITS).

1. Each Contractor requiring access to PROTECTED information must hold a valid RELIABILITY STATUS security clearance, granted by the Canadian Industrial Security Directorate (CISD) of Public Works and Government Services Canada (PWGSC).

2. Access to PROTECTED information shall not be provided to the Contractor's agents and subcontractors, volunteers, offenders or any other parties, unless those individuals have been authorized by CISD, hold a valid RELIABILITY STATUS security clearance and have a legitimate need-to-know for the information provided.

3. All of the Contractor's employees who are involved in this contract must be aware of their security obligations related to the handling of PROTECTED information.

4. Any computers used to store and/or process PROTECTED information shall be located in a space that meets the requirements of an Operations Zone as defined in the Treasury Board's Operational Security Standard on Physical Security.

5. If PROTECTED information is stored or processed on removable storage media such as a USB flash drives, the information must be protected by a strong password and encrypted using a product that meets Government of Canada (GC) encryption standards as defined in ITSA-11E CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within GC.

6. When not in use, all removable storage media shall be secured in a security container that meets GC security standards within an Operations Zone.

7. When PROTECTED information is being displayed on a computer screen or being viewed in printed format, it must not be viewable by unauthorized persons.

8. When sending PROTECTED information via email or other electronic exchange, it must be encrypted using a product or service that meets GC encryption standards as defined in ITSA-11E CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within GC.

9. All documentation produced or completed by the Contractor which contains PROTECTED information shall have its sensitivity labeled in the upper right hand corner on the face of each page of the document. Also, all removable storage media such as USB devices and backup tapes must be labelled with the sensitivity level of the information contained therein, e.g. PROTECTED.

10. On all computers used to store and/or process PROTECTED information, a password protected screen saver set to 5 minutes or less must be enabled.

11. On all computers used to store and/or process PROTECTED information, current antivirus software must be installed and maintained with the most current virus definitions and signatures.

IT Security Requirements Technical Document

IT Security, Correctional Service Canada

12. On all computers used to store and/or process PROTECTED information, the Operating System (OS) must be a vendor-supported OS (i.e. current security patches must still be available and the product not have reached end of life) and the most recent OS and applications security patches must be installed and updated with the most current version.

13. On all computers used to store and/or process PROTECTED information, access to the information must be restricted by requiring a unique user account ID and strong password for each user who will access the information or use the computer on which it sits. Computer accounts must not be shared.

14. Computer accounts with administrator privileges must only be used for system administration and should not have access to the Internet.

15. Security event logging must be enabled and logs kept for a minimum of 1 month.

16. All computers used to store and/or process PROTECTED information which are also connected to the Internet should reside behind a NAT-enabled firewall that is securely-configured using industry best practices (e.g. configuration documented; security logs enabled, maintained and reviewed; default denies all but required).

17. Remote access to the Information System, if required, must be securely-configured using industry best practices (e.g. ACLs, two-factor authentication, security logs, no split tunneling, VPN client provided by Contractor to employee and meeting requirements 10 to 15 above).

18. Connecting computers used to process PROTECTED information using wireless networks or wireless broadband Internet technologies is strongly discouraged and if inevitable, the wireless access must be securely-configured using industry best practices (e.g. router configured with WPA, not broadcasting SSID, using a strong password, changing the password every 6 months, with MAC filtering).

19. All PROTECTED information in the Contractor's custody shall be stored on physical computers and storage media in their custody and located in Canada only. The use of third-party cloud services (e.g. Google Drive, Dropbox) is prohibited.

20. Upon request of the client, the ability to immediately, securely and permanently wipe all PROTECTED information from any computers and removable storage media must be maintained.

21. Unless prescribed otherwise by law, all electronic devices used to store and/or process PROTECTED information such as computers, multi-function printers, photocopiers, removable storage media and other devices that contain hard disks, shall be sanitized or disposed of using security procedures defined in ITSG-06 to ensure no residual PROTECTED information can be read off these devices.

22. All individuals without a valid RELIABILITY STATUS security clearance must be directly supervised if/when they are to service or maintain a computer used to store and/or process PROTECTED information on the Contractor's premises to prevent unauthorized access to the information.

23. If there is a requirement to service a computer that is used to store and/or process PROTECTED information outside of the Contractor's premises, any hard disk(s) containing PROTECTED information must be removed and secured with the Contractor prior to the computer being removed from the premises.

IT Security Requirements Technical Document

IT Security, Correctional Service Canada

24. If it has been determined that a computer hard disk used to store and/or process PROTECTED information is no longer serviceable, the hard disk must be surrendered to the Project Authority for destruction.

25. Any loss or theft of PROTECTED information must be reported by the Contractor to the Project Authority within 2 *hours* of detection.

In addition, for contracts where a connectivity requirement has been identified in the SRCL (i.e. "yes" to question 11e), the following IT Security requirements must be met:

26. All computers that have access to OMS, or its ancillary applications, and CSC's email system must:
    a. be configured with a password protected BIOS
    b. be BIOS configured to only boot from C: drive
    c. have their wireless capability turned off

27. On all computers that have access to OMS, or its ancillary applications, and CSC's email system, the use of the following is prohibited:
    a. peer-to-peer software to communicate with other systems
    b. network based gaming software
    c. client-server software such as web server, proxy server, file server, etc. (Citrix Receiver allowed)
    d. webmail services (Outlook Web Access allowed)
    e. freeware and shareware (Contact CSC IT Security for possible exceptions)
    f. remote control software (SimpleHelp allowed)
    g. ftp client software