Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

**RETURN BIDS TO:**
**RETOURNER LES SOUMISSIONS À:**
**Bid Receiving - PWGSC / Réception des soumissions - TPSGC**
**11 Laurier St./ 11 rue, Laurier**
**Place du Portage, Phase III**
**Core 0B2 / Noyau 0B2**
**Gatineau, Québec K1A 0S5**
**Bid Fax: (819) 997-9776**

# SOLICITATION AMENDMENT
# MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

**Comments - Commentaires**
THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT / DOCUMENT CONTIENT DES EXIGENCES RELATIVES À LA SÉCURITÉ

**Vendor/Firm Name and Address**
**Raison sociale et adresse du fournisseur/de l'entrepreneur**

**Issuing Office - Bureau de distribution**
Scientific, Medical and Photographic Division / Division de l'équipement scientifique, des produits photographiques et pharmaceutiques
11 Laurier St./ 11 rue, Laurier
6A2, Place du Portage
Gatineau, Québec K1A 0S5

| | |
|---|---|
| **Title - Sujet**<br>AUTOMATED MEDICATION DISPENSING SYS | |
| **Solicitation No. - N° de l'invitation**<br>21120-180235/A | **Amendment No. - N° modif.**<br>002 |
| **Client Reference No. - N° de référence du client**<br>21120-18-2760235 | **Date**<br>2018-09-05 |
| **GETS Reference No. - N° de référence de SEAG**<br>PW-$$PV-915-75406 | |
| **File No. - N° de dossier**<br>pv915.21120-180235 | **CCC No./N° CCC - FMS No./N° VME** |
| **Solicitation Closes - L'invitation prend fin**<br>**at - à 02:00 PM**<br>**on - le 2018-10-10** | **Time Zone**<br>**Fuseau horaire**<br>Eastern Daylight Saving Time EDT |
| **F.O.B. - F.A.B.**<br>**Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐ | |
| **Address Enquiries to: - Adresser toutes questions à:**<br>MacCuaig, Shannon | **Buyer Id - Id de l'acheteur**<br>pv915 |
| **Telephone No. - N° de téléphone**<br>(873) 469-3983 ( ) | **FAX No. - N° de FAX**<br>( ) - |
| **Destination - of Goods, Services, and Construction:**<br>**Destination - des biens, services et construction:** | |

**Instructions: See Herein**

**Instructions: Voir aux présentes**

| | |
|---|---|
| **Delivery Required - Livraison exigée** | **Delivery Offered - Livraison proposée** |
| **Vendor/Firm Name and Address**<br>**Raison sociale et adresse du fournisseur/de l'entrepreneur**<br><br>**Telephone No. - N° de téléphone**<br>**Facsimile No. - N° de télécopieur** | |
| **Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)**<br>**Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)**<br><br>**Signature** **Date** | |

Canada

**Amendment 002 has been raised to add IT Security Requirements to the RFSO:**

INSERT: Annex E

Correctional Service Canada | Service correctionnel Canada

**UNCLASSIFIED / NON CLASSIFIÉ**

# IT Security Requirements Technical Document / Document technique – Exigences en matière de sécurité des TI

| | |
|---|---|
| **Contract # / N° de contrat :** | 21120-18-2760235 (NHQ2695) KW |
| **Date :** | 2018/01/09 KW |

(La version française suit)

## IT Security Requirements

The IT Security Requirements are derived from the Operational Security Standard: Management of Information Technology Security (MITS).

The requirements below apply to the above-noted contract and all contractors and external partners therein who access information of PROTECTED level sensitivity and use **PROTECTED IT Equipment** (refer to Appendix A: Definitions).

1. Any suspected loss or theft of PROTECTED IT Equipment containing PROTECTED information must be reported by the Contractor to the Project Authority immediately.

2. All PROTECTED IT Equipment must be located in a space that meets the requirements of an Operations Zone as defined in the Operational Security Standard on Physical Security and G1-026 Guide to the Application of Physical Security Zones.

3. All PROTECTED information in the Contractor's custody stored, processed and/or shared electronically must be encrypted using a product that meets Government of Canada (GC) encryption standards as defined in Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information and protected by a strong password (minimum 8 characters, uppercase letters, lowercase letters and numbers).

4. All PROTECTED information in the Contractor's custody must be stored in Canada only. Storage of all Government of Canada (GC) information outside Canada is prohibited. Only Canadian-based cloud storage services that are specifically-authorised by CSC may be used to store PROTECTED information; all other cloud services are prohibited.

5. Current antivirus software must be installed and enabled with the most current virus definitions, updates and maintained on all PROTECTED IT Equipment on which it is possible to install antivirus software.

6. The Operating System (OS) and applications used on PROTECTED IT Equipment must be vendor-supported, i.e. current security patches must be available and the product must not have reached end of life, and the latest security patches must be installed.

7. Each authorized user who accesses PROTECTED IT Equipment must use their own unique account with user-level privileges and protect it using a strong password. Computer accounts must not be shared. Computer accounts with Administrator-level privileges must be used for system administration tasks only and must not be used for general user tasks, e.g. surfing the Internet, checking email, accessing OMS.

8. Security event logging must be enabled and logs kept for a minimum of 1 month on all PROTECTED IT Equipment on which event logging is possible.

9. A password protected screen saver set to 15 minutes or less must be enabled on all PROTECTED IT Equipment connected to or including a digital display or monitor.

10. All PROTECTED IT Equipment that is connected to the Internet must reside behind a network router that is securely-configured using industry best practices, e.g. NAT-enabled firewall, password-protected and documented configuration, security logging enabled, maintained and reviewed, and filtered access.

11. When PROTECTED IT Equipment is no longer required to store or process PROTECTED information, the information stored on the equipment must be securely destroyed in accordance with IT Media Sanitization. Any PROTECTED information stored on approved Canadian-based cloud storage services must also be deleted when no longer needed.

12. All PROTECTED IT Equipment must have its internal data storage devices, e.g. hard drives, removed and secured with the Contractor prior to the equipment being removed from the Contractor's premises for service.

13. If it has been determined that PROTECTED IT Equipment is no longer serviceable, any internal data storage devices, e.g. hard drives, contained in the equipment must be surrendered to the Project Authority for destruction. If the internal storage cannot be removed from its host equipment, the host equipment itself must be surrendered to the Project Authority for destruction.

14. When PROTECTED information is displayed on the screens of PROTECTED IT Equipment or viewed in printed format, it must not be viewable by unauthorized persons.

15. Unless otherwise prohibited, any remote access to PROTECTED IT Equipment using Contractor-provided and/or CSC-provided standard remote access software must be secured using industry best practices, e.g. encrypted connection, two-factor authentication, controlled/restricted access, security logging, split tunneling disabled. All parties using the remote access must also meet all requirements listed in this document.

## Additional Security for Connectivity (and other External Partners)

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:

16. All PROTECTED IT equipment used to access Offender Management System (OMS), its ancillary applications or CSC's email system must meet the following requirements:

    a. The BIOS is protected with a strong password.
    b. The BIOS is configured to allow booting only from the system drive, e.g. C: drive.
    c. All wireless capability is disabled.
    d. The system is locked or shut down when not in use.

17. All PROTECTED IT equipment used to access OMS, its ancillary applications or CSC's email system must never have the following installed and/or used on the equipment unless specifically-authorised by CSC:

    a. Tools that could circumvent security controls.
    b. Peer-to-peer (P2P) software used to communicate with other systems over the Internet
    c. Client-server software such as web servers, proxy servers or file servers.
    d. Web-based email services.
    e. Remote-control software.
    f. Cloud services, including storage (see Requirement 4).

## Departmental Security – Physical and Personnel

In addition to the aforementioned items, compliance with the following items below is assumed through Designated Organization Screening (DOS) and Document Safeguarding Capability (DSC) verifications conducted by Canadian Industrial Security Directorate (CISD):

- Each Contractor, Contractor's agents, subcontractors, volunteers or any other parties requiring access to PROTECTED information must hold a valid RELIABILITY STATUS security clearance, granted by the CISD of Public Works and Government Services Canada (PWGSC) and have a legitimate need-to-know for the information provided.

- When not in use, all Portable Data Storage Devices containing PROTECTED information must be secured in a security container that meets GC security standards within an Operations Zone.

- All documentation produced or completed by the Contractor which contains PROTECTED information must have its sensitivity labeled in the upper right hand corner on the face of each page of the document. Also, all Portable Data Storage Devices must be labelled with the highest sensitivity level of the information contained therein, e.g. PROTECTED B.

# IT Security Requirements Technical Document / Document technique – Exigences en matière de sécurité des TI

## Appendix A: Definitions

**PROTECTED IT Equipment** - All Information Technology (IT) equipment and devices (such as, but not limited to, servers, desktop computers, Portable Data Storage Devices) that are used to access, store and/or process information of PROTECTED level sensitivity.

**Portable Data Storage Device (PDSD)** - Devices that are portable and contain storage or memory into which users can store information are considered portable data storage devices. Examples of portable data storage devices include:

- USB devices (e.g. memory sticks, external hard drives);
- eSATA (External Serial Advanced Technology Attachment) devices;
- Tablets, laptops, smart devices (e.g. BlackBerry), and cameras; and
- Portable media – tapes, optical discs (e.g. CDs and DVDs).

## Appendix B: References

- Operational Security Standard: Management of Information Technology Security (MITS)
  http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328
- Operational Security Standard on Physical Security
  http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329
- G1-026 - Guide to the Application of Physical Security Zones
  http://www.rcmp-grc.gc.ca/physec-secmat/pubs/g1-026-eng.htm
- Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information
  https://www.cse-cst.gc.ca/en/publication/itsp-40-111
- IT Media Sanitization
  https://www.cse-cst.gc.ca/en/publication/itsp-40-006v2
- G1-001 - Security Equipment Guide
  http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm



**All other terms and conditions of the RFSO remain unchanged.**