Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
21120-17-2521555
Security Classification / Classification de sécurité

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Correctional Services Canada	2. Branch or Directorate / Direction générale ou Direction: Community Reintegration Branch
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Suppliers are required to provide accommodation, monitoring, general support and assistance to offenders under federal jurisdiction who have been released to the community on conditional release, statutory release, and those subject to Long-Term Supervision Orders.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui

8. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?	☑ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada	☑	NATO / OTAN	☐	Foreign / Étranger	☐

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion: ☑	All NATO countries / Tous les pays de l'OTAN: ☐	No release restrictions / Aucune restriction relative à la diffusion: ☐
Not releasable / À ne pas diffuser: ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A	☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	☐	PROTECTED A / PROTÉGÉ A	☐
PROTECTED B / PROTÉGÉ B	☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	☐	PROTECTED B / PROTÉGÉ B	☐
PROTECTED C / PROTÉGÉ C	☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐	PROTECTED C / PROTÉGÉ C	☐
CONFIDENTIAL / CONFIDENTIEL	☐	NATO SECRET / NATO SECRET	☐	CONFIDENTIAL / CONFIDENTIEL	☐
SECRET / SECRET	☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET	☐	SECRET / SECRET	☐
TOP SECRET / TRÈS SECRET	☐			TOP SECRET / TRÈS SECRET	☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	☐			TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
21120-17-2521555
Security Classification / Classification de sécurité

PART A (continued) / PARTIE A (suite)

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :
☑ No / Non ☐ Yes / Oui

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?
☑ No / Non ☐ Yes / Oui

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☐ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET – SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
☑ No / Non ☐ Yes / Oui

If Yes, will unscreened personnel be escorted?
Dans l'affirmative, le personnel en question sera-t-il escorté?
☐ No / Non ☐ Yes / Oui

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?
☐ No / Non ☑ Yes / Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?
☑ No / Non ☐ Yes / Oui

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?
☑ No / Non ☐ Yes / Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?
☐ No / Non ☑ Yes / Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?
☑ No / Non ☐ Yes / Oui

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
21120-17-2521555
Security Classification / Classification de sécurité

PART C - (continued) / PARTIE C - (suite)

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens		✓														
Production																
IT Media / Support TI		✓														
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
21120-17-2521555
Security Classification / Classification de sécurité

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Richard Marceau	Branch Area Director	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613 992 2444	613-954-1687	Richard.c.marceau@csc..	2017/02/02

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Robert Wattie	Contract Security Analyst	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
(613) 415-8705		Robert.Wattie@csc-scc.gc.ca	Feb 3, 2017.

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?
No / Non ☐ Yes / Oui ☒

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Owen Nicholl	Sr. Procurement Officer	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-947-5219	—	Owen.Nicholl@csc.scc.gc.ca	Jan. 30/17

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

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

Contract # / N° de contrat :	21120-17-2521555
Date:	Feb 3, 2017.

(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 therein who access information of PROTECTED level sensitivity and use PROTECTED IT Equipment defined as: All Information Technology (IT) equipment and devices (such as, but not limited to, computers, laptops, USB flash drives, optical discs, memory cards, tablets) that are used to store and/or process information of PROTECTED level sensitivity.

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

2. All PROTECTED IT Equipment must 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.

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 ITSA-11E CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within GC 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 PROTECTED information outside Canada is prohibited. Only Canadian-based cloud storage services that are specifically-authorised by the department 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.

6. The Operating System (OS) of all computers used to store or process PROTECTED information 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 versions of OS and applications security patches must be installed.

7. Each authorized user who accesses PROTECTED IT Equipment must have use their own unique account with user-level privileges and protected by 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 to access the Internet.

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

9. A password protected screen saver set to 15 minutes or less must be enabled on all PROTECTED IT Equipment.

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. All PROTECTED IT Equipment must have its hard drives (and other internal storage) containing PROTECTED information removed and secured with the Contractor prior to the equipment being removed from the Contractor's premises for service.

12. If it has been determined that a hard drive used to store and/or process PROTECTED information is no longer serviceable, the hard drive must be removed from its host equipment and surrendered to the Project Authority for destruction.

13. When devices such as computer hard drives and portable data storage devices are no longer required to store or process PROTECTED information, the information must be securely destroyed in accordance with ITSG-06 Clearing and Declassifying Electronic Data Storage Devices. Any PROTECTED information stored on approved cloud storage services must also be deleted when no longer needed.

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

15. Any remote access to the Contractor's Information System and the PROTECTED information contained therein, including all remote connections to computers and other network devices, must be secured using industry best practices, e.g. encrypted connection, two-factor authentication, security logging, split tunneling disabled, access control lists, Contractor-provided and standard remote access software. Any party using the remote access must also meet all requirements listed in this document.

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 equipment that has access to OMS, its ancillary applications or CSC's email system must meet the following requirements:

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

17. All PROTECTED equipment that has access to OMS, its ancillary applications or CSC's email system must never have the following installed and/or used on the equipment:

    a. Hacking 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, except Citrix Receiver.
    d. Webmail services except Outlook Web Access to connect to CSC.
    e. Remote-control software (unless specifically-authorised by the department).
    f. Cloud services (e.g. Google Drive, Dropbox, Apple iCloud), unless specifically-authorised by the department (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 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 Canadian Industrial Security Directorate (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 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.

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

Exigences en matière de sécurité des technologies de l'information (TI)

Les présentes exigences en matière de sécurité des TI découlent de la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI).

Les exigences énoncées dans les paragraphes qui suivent s'appliquent au contrat précisé ci-dessus ainsi qu'à tous les entrepreneurs qui consultent des renseignements PROTÉGÉS ou utilisent de l'équipement de TI PROTÉGÉ. *Équipement de TI PROTÉGÉ* s'entend de l'ensemble du matériel et des appareils de TI (notamment, sans toutefois s'y limiter, les ordinateurs, les ordinateurs portables, les clés USB, les disques optiques, les cartes mémoire et les tablettes) servant à stocker ou à traiter des renseignements PROTÉGÉS.

1. L'entrepreneur doit signaler au chargé de projet toute perte ou tout vol soupçonné de renseignements PROTÉGÉS dans les *deux heures* suivant la détection.

2. Tout l'équipement de TI PROTÉGÉ doit se trouver dans un espace qui respecte les exigences d'une zone de travail, telle qu'elle est définie dans la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor.

3. Tous les renseignements PROTÉGÉS dont l'entrepreneur a la garde et qui sont stockés, traités ou transmis par voie électronique doivent être chiffrés à l'aide d'un produit conforme aux normes de chiffrement du gouvernement du Canada définies dans l'alerte de sécurité de la TI ITSA-11E, « Algorithmes cryptographiques approuvés par le Centre de la sécurité des télécommunications Canada (CSTC) pour la protection des renseignements sensibles et pour les applications d'authentification et d'autorisation électroniques au sein du GC ». Ils doivent également être protégés par un mot de passe robuste d'au moins huit caractères (majuscules, minuscules et chiffres).

4. Tous les renseignements PROTÉGÉS dont l'entrepreneur a la garde doivent être stockés au Canada uniquement. Le stockage de renseignements PROTÉGÉS à l'extérieur du Canada est interdit. Seuls des services de stockage infonuagiques basés au Canada et autorisés spécifiquement par le Service peuvent être utilisés pour stocker des renseignements PROTÉGÉS; tous les autres services infonuagiques sont interdits.

5. Sur tout l'équipement de TI PROTÉGÉ, un logiciel antivirus récent doit être installé et mis à jour avec les définitions de virus les plus récentes.

6. Le système d'exploitation (SE) du matériel informatique utilisé pour traiter des renseignements de nature délicate doit être appuyé par le vendeur, i.e. le produit ne doit pas être arrivé en fin de vie et les mises à jour les plus récentes doivent être disponibles. Le SE et les applications installées doivent utiliser les mises à jour les plus récentes.

7. Chaque utilisateur autorisé qui accède à de l'équipement de TI PROTÉGÉ doit posséder son propre compte unique doté de privilèges d'utilisateur et protégé par un mot de passe robuste. Il est interdit de partager les comptes informatiques. Les comptes informatiques dotés de privilèges d'administrateur doivent servir exclusivement à des tâches d'administration des systèmes et ne doivent pas donner accès à Internet.

8. Sur tout l'équipement de TI PROTÉGÉ, l'enregistrement d'événements de sécurité doit être activé et ces enregistrements doivent être conservés au moins un mois.

9. Sur tout l'équipement de TI PROTÉGÉ, un économiseur d'écran protégé par un mot de passe et réglé à 15 minutes ou moins doit être activé.

10. Tout l'équipement de TI PROTÉGÉ qui est branché sur Internet doit être connecté à un routeur configuré de façon sécuritaire conformément aux pratiques exemplaires de l'industrie (p. ex. pare-feu compatible avec la traduction d'adresse de réseau [NAT], protection par un mot de passe, configuration documentée, journal de sécurité activé, tenu à jour et passé en revue et filtrage des accès).

11. Sur tout l'équipement de TI PROTÉGÉ, les disques durs (et tout autre support de stockage interne) contenant des renseignements PROTÉGÉS doivent être retirés et mis en lieu sûr avec l'entrepreneur avant le retrait de l'équipement des locaux de l'entrepreneur aux fins d'entretien.

12. S'il a été déterminé qu'un disque dur utilisé pour traiter ou stocker des renseignements PROTÉGÉS n'est plus utilisable, le disque dur doit être retiré de l'équipement hôte, puis remis au chargé de projet en vue de sa destruction.

13. Lorsque des appareils (disques durs et supports de stockage de données portatifs, entre autres) ne sont plus requis pour traiter ou stocker des renseignements PROTÉGÉS, les renseignements doivent être éliminés de façon sécuritaire conformément au document ITSG-06 – Effacement et déclassification des supports d'information électroniques. Les renseignements PROTÉGÉS stockés au moyen de services infonuagiques autorisés doivent aussi être éliminés lorsqu'ils ne sont plus requis.

14. Si les renseignements PROTÉGÉS sont affichés sur un écran d'ordinateur ou consultés en format imprimé, ils ne doivent pas être visibles par des personnes non autorisées.

15. Tout accès à distance au système d'information de l'entrepreneur et aux renseignements PROTÉGÉS qu'il héberge, notamment toute connexion à distance aux ordinateurs et autres périphériques réseau, doit être sécurisé conformément aux pratiques exemplaires de l'industrie (p. ex. connexion chiffrée, authentification à deux facteurs, journal de sécurité, partage de tunnel désactivé, listes de contrôle d'accès, logiciel d'accès à distance standard fourni par l'entrepreneur). Toute partie recourant à l'accès à distance doit également répondre à toutes les exigences précisées dans le présent document.

De plus, en ce qui a trait aux contrats pour lesquels des exigences en matière de connectivité ont été énoncées dans la Liste de vérification des exigences relatives à la sécurité (c.-à-d. que l'on a répondu « oui » à la question 11e), les exigences en matière de sécurité des TI suivantes doivent être respectées :

16. Tout équipement PROTÉGÉ muni d'un accès au Système de gestion des délinquant(e)s (SGD), à ses applications auxiliaires ou au système de courriel du Service correctionnel du Canada (SCC) doit répondre aux exigences suivantes :

    a. protection du BIOS par un mot de passe;
    b. configuration du BIOS de façon à ne permettre le démarrage qu'à partir du lecteur C:;
    c. désactivation de toutes les fonctionnalités sans fil;
    d. verrouillage ou arrêt du système lorsqu'il n'est pas utilisé.

17. Ce qui suit ne doit en aucun cas être installé ou utilisé sur tout équipement PROTÉGÉ muni d'un accès au Système de gestion des délinquant(e)s (SGD), à ses applications auxiliaires ou au système de courriel du Service correctionnel du Canada (SCC) :

    a. outils de piratage qui pourraient contourner les contrôles de sécurité;
    b. logiciels poste-à-poste (P2P) servant à communiquer avec d'autres systèmes par Internet;
    c. logiciels client-serveur comme les serveurs Web, des serveurs mandataires ou des serveurs de fichiers, à l'exception de Citrix Receiver;
    d. services de messagerie Web, à l'exception d'Outlook Web Access pour se connecter au SCC;
    e. logiciels de commande à distance (excepté lorsqu'autorisé spécifiquement par le Service) ;
    f. services infonuagiques (p. ex., Google Drive, Dropbox, Apple iCloud), excepté lorsqu'autorisé spécifiquement par le Service (voir l'exigence nº 4).

Sécurité ministérielle – sécurité physique et personnelle

En plus des éléments susmentionnés, la Direction de la sécurité industrielle canadienne (DSIC) procédera à des vérifications d'organisation désignée (VOD) et à des vérifications de la cote de protection des documents (CPD) afin d'assurer le respect des exigences suivantes :

- Chaque entrepreneur, agent de l'entrepreneur, sous-traitant, bénévole ou toute autre partie qui demande l'accès à des renseignements PROTÉGÉS doit détenir une COTE DE FIABILITÉ valide, octroyée par la DSIC de Travaux publics et Services gouvernementaux Canada (TPSGC), et présenter un motif légitime de consulter les informations renseignements en question (besoin de savoir).

- Lorsqu'ils ne sont pas utilisés, tous les supports de stockage de données portatifs contenant des renseignements PROTÉGÉS doivent être mis en lieu sûr dans un coffre de sécurité répondant aux normes de sécurité du gouvernement du Canada, dans une zone de travail.

- Tous les documents produits ou remplis par l'entrepreneur qui contiennent des renseignements PROTÉGÉS doivent porter la mention affichant la cote de sécurité dans le coin supérieur droit de chaque page. De plus, tous les supports de stockage amovibles, comme les clés USB et les bandes de sauvegarde, doivent porter une étiquette de la cote de sécurité des renseignements qu'ils contiennent, p. ex., PROTÉGÉ.