Government of Canada / Gouvernement du Canada

RECEIVED
AOUT 19 2014
AUG

SRCL 1323-082014

Contract Number / Numéro du contrat
0,B68-14-0259
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: Agriculture and Agri-Food Canada

2. Branch or Directorate / Direction générale ou Direction: Corporate Management 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
Tax information slip System (TISS) - Generation, printing and mailing of tax slips for non-apy taxable benefits on behalf of AAFC, according to Canada Revenue Agency (CRA) and Revenue Québec (RQ) specifications

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

6. 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

Canada	NATO / OTAN	Foreign / Étranger
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

Canada	NATO	Foreign / Étranger
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
01B68-14-0259
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
01B69-14-0259
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 / TRES 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
01B68-14-0259
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
Manon Renaud	Chief, Accounts Receivables and Revenue	Manon Renaud

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-773-3186	613-773-0660	manon.renaud@agr.gc.ca	2014-07-31

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Lise Levesque-Masson	SRCL Coordinator	Lise Levesque-Masson

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-773-1464	613-773-1488	lise.levesque-masson@agr.gc.ca	Aug 5 2014

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? agr.gc.ca
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
Stephanie Sehn	Senior Contracting Officer	Stephanie Sehn

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-773-0935	613-773-0966	stephanie.sehn@agr.gc.ca	August 19, 2014

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Anna Kulycka Contract Security Officer, Contract Security Division Anna.Kulycka@tpsgc-pwgsc.gc.ca Tél. / Tel. - 613-957-1258 / Fax/Téléc - 613-954-4171		

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
			Sept 5, 2014

IT Security Requirements for the Processing, Storage and Transmittal of Protected B Information

Contract #:	01B68-14-0259
Department:	AAFC-AAC
Contractor/Supplier:	

1. INTRODUCTION

This document outlines the Department's IT Security requirements, in conjunction with any other Canadian Industrial Security Directorate (CISD) requirements, in support of the Contractor/Supplier obtaining an official CISD written approval to use their IT system to process and store Protected B information.

In 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 and storage of Protected B information be approved by the Department's IT Security Coordinator (ITSC).

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

2. MANDATORY PREREQUISITES

2.1. PWGSC Validation for Physical Security

The application of the security safeguards listed in this document are based on the *mandatory requirement* that the physical premises of the Contractor/Supplier have been inspected, certified and accredited to process and store Protected B information by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services. Hence, for the duration of this contract, the Contractor/Supplier must hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of Protected B issued by the CISD.

2.2. Personnel Security

All Contractor/Supplier personnel who have access to the material being processed and stored must hold a valid Government of Canada (GC) Reliability Check and Status or a Security Clearance and have the "*need to know*".

All of the Contractor/Supplier personnel handling Protected B information, in relation to this contract, must attend a mandatory security training/briefing session coordinated and delivered by the Contractor's/Supplier's appointed Company Security Officer or alternates.

2.3. Information Security

All hard copy documents and other media formats must be handled and transported in accordance with GC guidelines. All hard copy documents and other media will be marked

with the appropriate security classification. Any covering letter, transmittal form or circulation slip will be marked to indicate the highest level of classification of the attachments.

Transportation of information associated with this contract into or out of the physical premises must adhere to RCMP G1-009 "*Transport and Transmittal of Protected and Classified Information*". All processing and storage of Protected B information must be performed within the confines of CISD approved physical locations for this contract.

2.4. Security Policy Compliance Monitoring

The Department retains the right to conduct inspections of the Contractor/Supplier facility to ensure compliance with GC standards and policies with respect to the handling, storage and processing of information relevant to this contract.

3. MINIMUM IT SECURITY REQUIREMENTS

In conjunction with any other requirements established by the CISD, the Contractor/Supplier must meet the following IT Security requirements established by the Department.

Furthermore, the Contractor/Supplier must ensure that effective security controls are in place to protect medium level Confidentiality and Integrity and, at minimum, medium level Availability. Communications Security Establishment Canada's (CSEC's) recommendations and guidelines must be followed. Their published ITSG-33 documentation will provide further details.

3.1. IT Security Policy Compliance and Monitoring

All information technology related operations must adhere to the overall requirements outlined in the GC's Operational Security Standard: Management of Information Technology Security (MITS). All IT Security requirements addressed to the Department are applicable to the Contractor/Supplier.

The Department retains the right to conduct inspections of the Contractor/Supplier facility to ensure compliance with GC policies and standards with respect to requirements in the Operational Security Standard: Management of Information Technology Security.

3.2. Prevention

As per MITS section 16, the Contractor/Supplier must have all the prevention safeguards in place for the protection of confidentiality, integrity, and availability of the information and IT assets relative to this contract.

3.2.1 Physical Security within the IT Security Environment

Along with providing official assurance that the CISD has approved its facilities to process and store Protected B information, the Contractor/Supplier must ensure that all equipment used for the fulfilment of this contract reside within the CISD approved physical locations.

The Contractor/Supplier must protect all equipment being used for this contract. The use of wireless technology must be approved by the Communications Security Establishment of Canada (CSEC) for the information's level of sensitivity and follow guidance in CSEC's ITSPSR-21A.

3.2.2 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 B information relative to this contract must be identified and labelled accordingly.

In the event of failure and replacement of the equipment or upon termination of the contract, all devices or material must be retained and properly stored or disposed of according to CSEC recommendations. The Contactor/Supplier is also responsible for clearing and sanitizing all electronic data storage devices used for this contract according to CSEC's ITSG-06 guideline.

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 unless it has been cleared or sanitized according to CSEC recommendations found in the ITSG-06 guideline.

All media, when not in use, must be stored in a storage container which is RCMP-approved for the storage of Protected B information (G1-001 "*Security Equipment Guide*"). The storage container must be verified by the CISD.

3.2.3 Authorization and Access Control

The Contractor/Supplier must restrict IT and information access relative to this contract only to its individuals who have been screened and authorized, have been identified and authenticated, and have a "need to know".

In following the 'principle of least-privilege', the Contractor/Supplier must provide only the minimum access required for individuals to perform their duties.

The Contractor/Supplier must withdraw all access privileges relative to this contract from individuals no longer involved.

3.2.4 Cryptography, Network Security and Perimeter Defence

The electronic storage of Protected B information associated with this contract must be within a CISD approved IT environment.

Electronic transmission of Protected B information must be encrypted using CSEC approved technology such as Entrust Security Provider and the GC Public Key Infrastructure.

The Contractor/Supplier must segregate its networks into IT security zones and implement perimeter defence and network security safeguards. CSEC provides the ITSG-38 and ITSG-22 guidelines on this specific subject. As well, the Contractor/Supplier must apply strict control of all access to the protected zone where the information associated with this contract resides. Network perimeter defence safeguards (e.g. firewalls, routers) must be used to mediate all traffic and to protect servers that are accessible from the internet. The Contractor/Supplier is recommended to use CSEC encryption technology or its equivalent to ensure confidentiality, integrity, authentication and non-repudiation

The Need-to-Know principle must be applied and transmission must be restricted only to CISD approved recipients.

3.2.5 Mobile Computing and Teleworking

All processing and storage of Protected B information must be performed within the confines of the CISD approved physical locations for this contract.

3.2.6 Software Integrity and Security Configuration

The Contractor/Supplier should configure the security of their operating systems and application software being used to process Protected B information in accordance with security best practices (such as the Microsoft Security Compliance Toolkits for servers and clients). Safeguards must be implemented to "harden" servers and workstations processing Protected B information. For more information on software hardening and configuration best practices, refer to the best practices issued by CSEC, by the National Institute for Standards and Technology (NIST) and by the Center for Internet Security.

3.2.7 Malicious Code

The Contractor/Supplier must install, use and regularly update antivirus software and conduct scans on all electronic files from external systems.

3.3. Detection

It is important to have the ability to detect security related issues within the operating environment. The rigor and extent of detection must be based on a medium level of risk. To protect the information associated with this contract and ensure service delivery, the Contractor/Supplier must continuously monitor system performance to rapidly detect:

- Attempts (failed or successful) to gain unauthorized access to a system, or to bypass security mechanisms.
- Unauthorized probes or scans to identify system vulnerabilities.
- Unplanned disruption of systems or services.
- Denial-of-service attacks
- Unauthorized changes to system hardware, firmware, or software.
- System performance anomalies, and
- Known attack signatures.

At minimum, the Contractor/Supplier must include a security audit log function in all IT systems.

3.4. Response and Recovery

3.4.1 Incident Response

The Contractor/Supplier must establish mechanisms to respond effectively to IT incidents and exchange incident-related information with the Department immediately. The Contractor/Supplier must have a documented incident response process.

3.4.2 Incident Reporting

It is paramount that the Department is made aware of any security-related incidents with respect to the facilities and equipment used to process and store Protected B information associated with this contract.

The Contractor/Supplier must report any security-related incidents to the Department within *two hours* of an incident being detected or reported.

3.4.3 Recovery

Before reconnecting or restoring services, the Contractor/Supplier must ensure that all malicious software has been removed and that there is no potential for recurrence or spread.

With regards to the information associated with this contract, the Contractor/Supplier must:

- Back up the data regularly
- Test backups regularly to ensure that they can be used for recovery
- Back up all software and configuration data
- Facilitate the restoration of data and services by allowing systems to undo operations and return to an earlier state.
- Test restoration procedures regularly to ensure that they are effective and that they can be completed within the time allotted for recovery.
- Determine retention periods for essential business information and archived backups, and
- Ensure that off-site backup storage is within a CISD approved location if no CSEC approved encryption is being used.

Note that system recovery should be conducted in a manner that preserves the integrity of evidence, in the event of a criminal investigation of a security breach, for example.

4. CONCLUSION

In absence of a formal TRA, this document has established the Department's basic IT Security requirements for the processing and storage of up to and including Protected B information.

Through the Canadian Industrial Security Directorate's invaluable input and expertise at certifying that the Contractor/Supplier has met all IT Security requirements, the Department will be reassured that risks have, most likely, been mitigated to acceptable levels.

Exigences en matière de sécurité des technologies de l'information (TI) pour le traitement, le stockage et la transmission de renseignements désignés « Protégé B »

N° du contrat :	01B68-14-0259
Ministère :	AAFC-AAC
Entrepreneur/fournisseur :	

1. INTRODUCTION

Le présent document décrit les exigences du Ministère en matière de sécurité des technologies de l'information (TI) qui doivent être respectées de concert avec toute autre exigence de la Direction de la sécurité industrielle canadienne (DSIC), lorsque l'entrepreneur/le fournisseur obtient l'autorisation écrite officielle de la DSIC d'utiliser ses systèmes de TI pour traiter et stocker des renseignements désignés « Protégé B ».

Puisqu'il n'y a aucune évaluation de la menace et des risques (EMR) officielle et que les exigences de l'autorisation de sécurité relatives aux TI sont particulières au contrat, le document vise à énoncer les mécanismes de sécurité minimums nécessaires pour que le traitement et le stockage des renseignements désignés « Protégé B » soient approuvés par le coordonnateur de la sécurité des TI (CSTI) du Ministère.

La sécurité repose sur diverses protections. En d'autres termes, pour que les exigences en matière de sécurité des TI puissent protéger l'information efficacement, d'autres mécanismes et politiques de sécurité doivent les sous-tendre. Des mesures de protection des lieux, du personnel et de l'information, conformes à la Politique sur la sécurité du gouvernement et aux normes connexes de sécurité des TI, doivent avoir été mises en place avant la mise en œuvre de mécanismes de sécurité des TI.

2. EXIGENCES PRÉALABLES OBLIGATOIRES

2.1. Validation de la sécurité des lieux par TPSGC

L'application des mécanismes de sécurité énoncés dans ce document est fondée sur l'*exigence obligatoire* selon laquelle la DSIC du ministère des Travaux publics et des Services gouvernementaux (TPSGC) doit avoir inspecté et certifié les installations de l'entrepreneur/du fournisseur en vue du traitement et du stockage de renseignements désignés « Protégé B ». Par conséquent, pour la durée du contrat, l'entrepreneur/le fournisseur doit détenir une vérification d'organisation désignée (VOD) valide et une autorisation de garder des documents désignés « Protégé B » délivrées par la DSIC.

2.2. Sécurité du personnel

Tous les membres du personnel de l'entrepreneur/du fournisseur ayant accès aux données traitées et stockées auront une cote de fiabilité ou une autorisation de sécurité du gouvernement du Canada valide, ainsi que le « *besoin de savoir* ».

Tous les membres du personnel de l'entrepreneur/du fournisseur manipulant des renseignements désignés « Protégé B », dans le cadre du présent contrat, suivront un atelier obligatoire de formation ou d'information sur la sécurité, coordonné et animé par l'agent de sécurité d'entreprise désigné de l'entrepreneur/du fournisseur ou ses remplaçants.

2.3. Sécurité de l'information

Tous les documents en format papier et sur d'autres supports doivent être manipulés et transportés conformément aux lignes directrices du gouvernement du Canada. Il faut y indiquer le niveau de classification de sécurité applicable. Les lettres et les formules d'accompagnement, ainsi que les bordereaux de circulation doivent être annotés de manière à indiquer le niveau le plus élevé de classification des pièces jointes.

Le transport de renseignements liés au présent contrat à destination ou en provenance des installations physiques doit être conforme au guide G1-009 « *Transport et transmission de renseignements protégés ou classifiés* » de la Gendarmerie royale du Canada (GRC). Le traitement et le stockage de renseignements désignés « Protégé B » seront effectués dans les installations approuvées par la DSIC pour ce contrat.

2.4. Vérification de la conformité aux politiques de sécurité

Le Ministère se réserve le droit d'inspecter les installations de l'entrepreneur/du fournisseur afin de vérifier la conformité des installations aux normes et aux politiques du gouvernement du Canada concernant la manipulation, le stockage et le traitement de renseignements pertinents à ce contrat.

3. EXIGENCES MINIMALES EN MATIÈRE DE SÉCURITÉ DES TI

De concert avec toute autre exigence établie par la DSIC, l'entrepreneur/le fournisseur doit respecter les exigences en matière de sécurité des TI fixées par le Ministère et décrites ci-après.

De plus, l'entrepreneur/le fournisseur s'assurera que des mesures de contrôle efficaces en matière de sécurité sont en place pour protéger la confidentialité et l'intégrité (niveau moyen) et, au moins, la disponibilité (niveau moyen). Les recommandations et les lignes directrices du Centre de la sécurité des télécommunications Canada (CSTC) doivent aussi être respectées. La documentation ITSG-33 publiée par le CSTC fournit de plus amples renseignements.

3.1. Conformité aux politiques en matière de sécurité des TI et vérification connexe

Toutes les opérations liées aux TI se dérouleront conformément à l'ensemble des exigences énoncées dans la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du gouvernement du Canada. Toutes les exigences en matière de sécurité des TI applicables au Ministère s'appliquent aussi à l'entrepreneur/au fournisseur.

Le Ministère se réserve le droit d'inspecter les installations de l'entrepreneur/du fournisseur afin de vérifier la conformité des installations aux normes et aux politiques du gouvernement du Canada concernant les exigences contenues dans la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information.

3.2. Prévention

Conformément à la section 16 de la GSTI, l'entrepreneur/le fournisseur doit avoir les mesures de prévention nécessaires pour protéger la confidentialité, l'intégrité et la disponibilité de l'information et des biens de TI liés à ce contrat.

3.2.1 Sécurité des lieux de l'environnement de sécurité des TI

En plus de fournir la preuve officielle que la DSIC a approuvé ses installations pour le traitement et le stockage des renseignements désignés « Protégé B », l'entrepreneur/le fournisseur s'assurera que tout le matériel utilisé pour exécuter le contrat se trouve dans les installations approuvées par la DSIC.

L'entrepreneur/le fournisseur protégera tout le matériel utilisé dans le cadre du contrat. L'utilisation de la technologie sans fil doit être approuvée par la sécurité des télécommunications du Canada (CSTC) pour le niveau de sensibilité de l'information et le suivi des conseils dans ITSPSR-21A du CSTC.

3.2.2 Stockage, élimination et destruction des supports de TI

Les CD et les DVD, les clés USB, les disques durs de poste de travail, les disques durs de serveur, les bandes de sauvegarde et les autres dispositifs servant au traitement ou au stockage de renseignements désignés « Protégé B » liés à ce contrat doivent être identifiés et étiquetés de façon adéquate.

En cas de défaillance et de remplacement du matériel ou à la résiliation du contrat, tous les appareils ou dispositifs doivent être conservés et adéquatement stockés ou éliminés conformément aux recommandations du CSTC. L'entrepreneur/le fournisseur est également responsable de l'écrasement et du nettoyage de tous les supports d'information électroniques utilisés dans le cadre du contrat, conformément aux lignes directrices ITSG-06 du CSTC.

Si le matériel nécessite un entretien ou un soutien technique ou s'il doit être remplacé, le matériel informatique associé au traitement ou au stockage de renseignements protégés ne peut pas être confié à un fournisseur externe, sauf s'il a été écrasé ou nettoyé conformément aux recommandations du CSTC figurant dans les lignes directrices ITSG-06.

Lorsqu'ils ne sont pas utilisés, les supports doivent être placés dans un contenant approuvé par la GRC pour le stockage de renseignements désignés « Protégé B » (voir le guide G1-001 intitulé *Guide d'équipement de sécurité*). Le contenant en question doit faire l'objet d'une vérification par la DSIC.

3.2.3 Autorisation et contrôle de l'accès

L'entrepreneur/le fournisseur restreindra l'accès aux TI et aux renseignements visés par le contrat aux personnes qui ont été contrôlées et autorisées, qui ont été identifiées et authentifiées et qui ont le « besoin de savoir ».

Selon le principe du « droit d'accès minimal », l'entrepreneur/le fournisseur doit limiter l'accès au minimum nécessaire pour l'accomplissement des tâches.

L'entrepreneur/le fournisseur retirera les privilèges d'accès liés à ce contrat aux personnes qui ne participent plus au contrat.

3.2.4 Cryptographie, sécurité des réseaux et défense du périmètre

Le stockage électronique de renseignements désignés « Protégé B » associés au contrat doit être fait dans un environnement de TI approuvé par la DSIC.

Lorsqu'ils sont transmis par voie électronique, les renseignements désignés « Protégé B » seront chiffrés au moyen d'une technologie approuvée par le CSTC, comme Entrust Security Provider et l'infrastructure à clés publiques du gouvernement du Canada.

L'entrepreneur/le fournisseur séparera ses réseaux en zones de sécurité des TI et mettra en place des mesures de défense du périmètre et de sécurité des réseaux. Le CSTC a établi les lignes directrices ITSG-38 et ITSG-22 à ce propos. De plus, l'entrepreneur/le fournisseur doit appliquer un contrôle strict sur l'accès à la zone protégée où se trouve l'information associée au contrat. Des mesures de défense du périmètre des réseaux (p. ex. pare-feux ou routeurs) seront utilisées pour faciliter le trafic et protéger les serveurs accessibles à partir d'Internet. L'entrepreneur / fournisseur est recommandé d'utiliser la technologie de cryptage CSTC ou son équivalent pour assurer la confidentialité, l'intégrité, l'authentification et la non-répudiation. Le principe du besoin de savoir doit s'appliquer et les renseignements ne doivent être transmis qu'aux destinataires approuvés par la DSIC.

3.2.5 Informatique mobile et télétravail

Le traitement et le stockage des renseignements désignés « Protégé B » doivent être effectués dans les installations approuvées par la DSIC pour ce contrat.

3.2.6 Intégrité des logiciels et mesures de sécurité

L'entrepreneur/le fournisseur configurera ses systèmes d'exploitation et logiciels d'application servant au traitement des renseignements désignés « Protégé B » conformément aux pratiques exemplaires en matière de sécurité (comme les trousses d'outils Microsoft Security Compliance Manager pour les serveurs et les clients). Des mécanismes de sécurité doivent être mis en œuvre pour « renforcer » les serveurs et les postes de travail liés au traitement de renseignements désignés « Protégé B ». Pour plus

de détails sur les pratiques exemplaires de configuration et de renforcement des logiciels, prière de se reporter aux pratiques exemplaires émises par le CSTC, le National Institute for Standards and Technology (NIST) et le Centre for Internet Security.

3.2.7 Programmes malveillants

L'entrepreneur/le fournisseur doit installer et utiliser un logiciel antivirus et le mettre à jour régulièrement. Il doit également veiller à balayer tous les fichiers électroniques provenant de systèmes externes.

3.3. Détection

Il est important d'être en mesure de détecter les menaces à la sécurité de l'environnement. La rigueur et l'étendue de la détection seront fondées sur un niveau de risque moyen. Dans le but de protéger l'information relative au contrat et d'assurer la prestation des services, l'entrepreneur/le fournisseur doit surveiller continuellement le rendement des systèmes pour détecter rapidement :

- les tentatives (réussies ou non) d'accéder sans permission à un système ou de contourner les mécanismes de sécurité;
- les sondes ou les explorations non autorisées visant à déceler les vulnérabilités d'un système;
- les interruptions imprévues des systèmes ou des services;
- les attaques entraînant un déni de service;
- la modification non autorisée du matériel, des micrologiciels ou des logiciels;
- les anomalies du rendement d'un système;
- les signatures d'attaque connues.

Au minimum, l'entrepreneur/le fournisseur doit inclure une fonction de journal de vérification de la sécurité dans tous les systèmes de TI.

3.4. Réaction et reprise

3.4.1 Réaction aux incidents

L'entrepreneur/le fournisseur établira des mécanismes afin de répondre efficacement aux incidents de TI et d'échanger immédiatement des renseignements sur les incidents avec le Ministère. L'entrepreneur/le fournisseur doit avoir un processus de réaction aux incidents en place, ainsi que la documentation connexe.

3.4.1 Déclaration d'incidents

Il est extrêmement important d'aviser le Ministère d'un incident de sécurité concernant les installations et le matériel utilisés pour traiter et stocker des renseignements désignés « Protégé B » relatifs au contrat.

L'entrepreneur/le fournisseur déclarera tout incident de sécurité au Ministère dans les *deux heures* suivant sa détection ou son signalement.

3.4.3 Reprise

Avant de reconnecter ou de rétablir les services, l'entrepreneur/le fournisseur doit faire en sorte que tout le logiciel malveillant a été supprimé et qu'il n'y a aucun risque de répétition ou de propagation.

En ce qui concerne l'information liée au contrat, l'entrepreneur/le fournisseur doit :

- enregistrer les données régulièrement;
- vérifier régulièrement si les copies de sauvegarde peuvent servir à la reprise;
- faire des sauvegardes de toutes les données de logiciel et de configuration;
- faciliter la restauration des données et des services en permettant aux systèmes d'annuler des opérations et de revenir à un stade antérieur;
- mettre à l'essai régulièrement les procédures de restauration pour s'assurer qu'elles sont efficaces et qu'elles peuvent être réalisées dans le temps imparti pour la reprise;
- fixer les délais de conservation pour les données essentielles sur les activités et les copies de sauvegarde archivées;
- s'assurer que l'installation de sauvegarde hors site est approuvée par la DSIC si aucune technologie de chiffrement approuvée par le CSTC n'est utilisée.

À noter que la remise en état d'un système devrait être menée de façon à préserver l'intégrité de la preuve, par exemple, dans le cas d'une enquête criminelle d'une infraction à la sécurité.

4. CONCLUSION

En l'absence d'une EMR officielle, le présent document énonce les exigences de base du Ministère en matière de sécurité des TI pour le traitement et le stockage de renseignements désignés jusqu'au niveau « Protégé B » inclusivement.

Grâce à la contribution et au savoir-faire précieux de la DSIC qui permettent de certifier que l'entrepreneur/le fournisseur respecte toutes les exigences en matière de sécurité des TI, le Ministère s'assurera que les risques ont probablement été atténués et sont de niveau acceptable.