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 :	
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.