Exigences en matière de sécurité des marchés – Protégé B

1. INTRODUCTION

Le présent document explique les exigences en matière de sécurité de la TI que l'entrepreneur doit respecter avant le traitement de données de nature sensible d'un niveau *Protégé B* ou inférieur. En l'absence d'une évaluation de la menace et des risques (EMR) officielle, et en raison de la part de la TI de la cote de sécurité étant propre au marché, l'intention de ce document est d'énoncer les mesures de protection minimales requises de l'entrepreneur afin que le traitement de renseignements de nature sensible soit approuvé par la Direction de la sécurité industrielle canadienne (DSIC) de Services publics et Approvisionnement Canada (SPAC).

La sécurité est fondée sur des couches de protection; c'est-à-dire qu'afin que les exigences en matière de sécurité de la TI (STI) protègent de manière efficace les renseignements, elles doivent être précédées et appuyées par d'autres aspects de sécurité et les politiques connexes. Les mesures de protection de la sécurité physique, du personnel et de l'information, conformément à la Politique sur la sécurité du gouvernement et aux normes relatives à la STI, doivent exister *avant* la mise en œuvre des mesures de protection de la STI.

2. PRÉALABLES OBLIGATOIRES

2.1 **Validation de SPAC pour la sécurité physique**

L'application des mesures de protection de la sécurité énumérées dans ce document est fondée sur *l'exigence obligatoire* que les lieux physiques aient été inspectés par la DSCI de SPAC. Le bureau de l'agent de sécurité du Ministère (ASM) validera l'attestation et en avisera le coordonnateur de la sécurité de la TI.

2.2 **Sécurité du personnel**

Tous les membres du personnel qui ont accès au matériel traité doivent détenir une cote de sécurité valide du gouvernement du Canada au niveau approprié (dicté par le degré de sensibilité du matériel) et avoir un « *besoin de savoir* ».

Tous les membres du personnel de l'entrepreneur qui traitent des renseignements de nature sensible du gouvernement du Canada doivent suivre une formation ou une séance d'information coordonnée et présentée par le coordonnateur de la sécurité de la TI de l'ASM du Secrétariat du Conseil du Trésor du Canada.

2.3 **Autorisation et contrôle de l'accès**

L'entrepreneur doit fournir au coordonnateur de la sécurité de la TI du Secrétariat du Conseil du Trésor du Canada une liste de toutes les personnes qui ont accès aux renseignements de nature sensible traités pour le Ministère, ainsi que les politiques et les procédures actuelles de l'entrepreneur pour l'ajout de personnes dans l'environnement et le processus suivi lorsqu'une personne est retirée de l'environnement.

En suivant le principe de « droit d'accès minimal », l'entrepreneur doit accorder seulement l'accès minimum requis pour permettre aux personnes de s'acquitter de leurs tâches.

2.4 Sécurité de l'information

Tous les documents papier et autres formats de média doivent être manipulés et transportés conformément aux lignes directrices du gouvernement du Canada. Tous les documents papier et les autres médias seront marqués avec la classification de sécurité appropriée fournie par le Secrétariat du Conseil du Trésor du

Canada. Toute lettre couverture, formulaire de transmission ou feuillet de circulation sera marqué afin d'indiquer le niveau le plus élevé de classification des documents joints.

Le transport des renseignements associés à ce marché à l'intérieur ou à l'extérieur des lieux physiques doit respecter le guide G1-009 *« Transport et transmission de renseignements protégés ou classifiés »* de la Gendarmerie royale du Canada (GRC).
Les membres du personnel de l'entrepreneur peuvent seulement transporter les documents associés à ce marché à l'intérieur ou à l'extérieur du domaine physique Protégé B de la sécurité périmétrique du milieu de travail avec l'approbation de l'ASM du Secrétariat du Conseil du Trésor du Canada.

2.5 Surveillance de la conformité aux politiques de sécurité

À une fréquence à déterminer par l'agent de sécurité du Ministère ou le coordonnateur de la sécurité de la TI, le Secrétariat du Conseil du Trésor du Canada se réserve le droit de mener des inspections des installations de l'entrepreneur afin d'assurer la conformité aux normes et aux politiques du gouvernement du Canada relatives à la manipulation, à l'entreposage et au traitement de renseignements de nature sensible.

3. EXIGENCES MINIMALES DE SÉCURITÉ (DÉTAILS)

3.1 Sécurité physique

L'entreprise doit fournir ou prouver qu'elle détient ce qui suit :

- une brève description du rôle de l'organisation et de ses installations;
- des consignes de sécurité d'entreprise signées;
- un registre de contrôle du matériel pour les renseignements et les biens protégés;
- un registre de contrôle des visiteurs pour les renseignements et les biens protégés;
- un plan détaillé de l'étage signé indiquant la zone d'accueil et la zone de travail; le plan doit inclure toutes les entrées (portes et fenêtres) et l'emplacement de l'ensemble de l'équipement utilisé pour produire, stocker, détruire ou transmettre les données;
- des photos des zones, des portes, des fenêtres, des armoires, des déchiqueteuses et de l'équipement de TI;
- des contenants approuvés par la GRC pour entreposer les renseignements aux niveaux Protégé A et Protégé B;
- un équipement de destruction approuvé par la GRC ou le nom d'une entreprise de déchiquetage qui est autorisée au niveau approprié;
- une organisation de nettoyage ayant la cote de sécurité appropriée ou le nettoyage effectué sous supervision au cours des heures normales de travail.

3.2 Sécurité du personnel

- Toutes les personnes doivent détenir une cote de fiabilité valide ou supérieure.
- Le maintien de cette cote est requis pour la durée du contrat.

3.3 Sécurité de la TI

- Toute perte ou tout vol de renseignements PROTÉGÉS doit être signalé par l'entrepreneur à l'autorité de projet à l'intérieur d'un délai de 2 heures suivant la détection.
- Tout ordinateur utilisé pour stocker ou traiter des renseignements PROTÉGÉS doit être situé dans un espace qui satisfait aux exigences d'une zone de travail comme le définit la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor.
- Si des renseignements PROTÉGÉS sont stockés ou traités dans des dispositifs de stockage portatifs, comme des clés USB, les renseignements doivent être protégés par un mot de passe robuste et chiffrés au moyen d'un produit qui satisfait aux normes de chiffrement du gouvernement du Canada (GC), comme le définit la norme 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.
- Lorsque des renseignements PROTÉGÉ B sont envoyés électroniquement par courriel ou autre moyen d'échange électronique, ils doivent être protégés par un mot de passe robuste et chiffrés au moyen d'un produit ou d'un service qui satisfait aux normes de chiffrement du gouvernement du Canada (GC), comme le définit la norme ITSA-11E, Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements sensibles et pour les applications d'authentification et d'autorisation électroniques au sein du G.
- Tous les renseignements PROTÉGÉS sous la garde de l'entrepreneur doivent être stockés dans des ordinateurs et des médias de stockage physiques en sa possession et situés au Canada seulement. Il est interdit d'utiliser des services infonuagiques de tiers (par exemple, Google Drive, Dropbox) pour stocker des renseignements PROTÉGÉS.
- Sur tous les ordinateurs utilisés pour stocker ou traiter des renseignements PROTÉGÉS :
    - un logiciel antivirus à jour doit être installé et maintenu avec les définitions et les signatures de virus les plus récentes;
    - le système d'exploitation (SE) doit être pris en charge par le fournisseur (c'est-à-dire que des correctifs de sécurité à jour doivent être disponibles et le produit ne doit pas avoir atteint sa fin de vie utile), les correctifs de sécurité du SE et des applications les plus récents doivent être installés et le SE doit être mis à jour avec la version la plus récente;
    - l'accès aux renseignements doit être restreint en exigeant un ID de compte d'utilisateur unique et un mot de passe robuste pour chaque utilisateur qui consultera les renseignements ou utilisera l'ordinateur dans lequel ils résident;
    - les comptes de l'ordinateur ne doivent pas être partagés;
    - un économiseur d'écran protégé par mot de passe configuré pour un délai d'inactivité de 15 minutes ou moins doit être activé.
- Tous les ordinateurs utilisés pour stocker ou traiter des renseignements PROTÉGÉS, et qui sont également connectés à Internet, devraient se trouver derrière un routeur qui est configuré de manière sécurisée au moyen des pratiques exemplaires de l'industrie (par exemple, un pare-feu compatible NAT, une configuration protégée par mot de passe et documentée, le journal de sécurité activé, maintenu et examiné, l'accès filtré).
- La journalisation des événements de sécurité doit être activée et les journaux doivent être conservés pour un minimum de 90 jours.
- S'il est nécessaire d'effectuer l'entretien d'un ordinateur utilisé pour stocker ou traiter des renseignements PROTÉGÉS à l'extérieur des lieux de l'entrepreneur, tout disque dur contenant des renseignements

PROTÉGÉS doit être retiré et sécurisé par l'entrepreneur avant que l'ordinateur soit retiré des lieux.

- Si l'on détermine que le disque dur d'un ordinateur utilisé pour stocker ou traiter des renseignements PROTÉGÉS n'est plus fonctionnel, le disque dur doit être remis à l'autorité de projet afin d'être détruit.
- Lorsque des dispositifs comme des disques durs d'ordinateurs, des clés USB et tout autre dispositif utilisé pour stocker ou traiter des renseignements PROTÉGÉS ne sont plus requis pour stocker ou traiter les renseignements, les renseignements doivent être supprimés de manière sécurisée et l'espace libre restant sur le dispositif doit être effacé de manière sécurisée conformément aux pratiques exemplaires de l'industrie.
- Lorsque des renseignements PROTÉGÉS sont affichés sur un écran d'ordinateur ou consultés en format imprimé, ils ne doivent pas être visibles à des personnes non autorisées.
- Si l'accès à distance au système d'information de l'entrepreneur (c'est-à-dire les ordinateurs et les dispositifs de stockage) et aux renseignements PROTÉGÉS contenus dans celui-ci est requis, la configuration d'accès à distance doit être configurée de manière sécurisée au moyen des pratiques exemplaires de l'industrie (par exemple, connexion chiffrée, authentification à deux facteurs, journalisation de la sécurité, aucune tunnellisation partagée, listes de contrôle d'accès, logiciel d'accès à distance fourni par l'entrepreneur à l'employé).
    - Tout employé qui utilise l'accès à distance doit également satisfaire à toutes les exigences énumérées dans ce document en ce qui a trait à son emplacement à distance et à l'équipement utilisé à cet endroit.