ANNEXE D

Contrôles de sécurité de la TI

Présentation

Le présent document souligne les exigences relatives à la sécurité de la TI liées au contrat nº _____de la Commission d'examen des plaintes concernant la police militaire du Canada (CPPM) pour le traitement de données sensibles jusqu'au niveau Protégé B inclusivement. Conformément à l'évaluation de la menace et des risques et parce que les exigences pour les TI visant l'autorisation de sécurité varient selon le contrat, ce document vise à présenter les mesures de sécurité minimales nécessaires pour que le traitement des renseignements sensibles soit approuvé par le coordonnateur de la sécurité des TI de la CPPM; Bruno Prévost, au numéro de téléphone 343-543-2609, à l'adresse courriel : bruno.prevost@mpcc-cppm.gc.ca.

La sécurité repose sur diverses protections. En d'autres termes, les exigences de sécurité pour les TI, lorsqu'elles sont respectées, permettent de protéger efficacement l'information seulement si d'autres mesures et politiques de sécurité les sous-tendent. Les 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 pour les TI, doivent avoir été mises en application avant la mise en œuvre d'exigences de sécurité pour les TI.

1. Exigences préalables obligatoires

1.1 Validation de la sécurité des lieux

L'application des mesures de sécurité énoncées dans le présent document est conditionnelle à l'inspection et à la certification obligatoires des lieux en vue du traitement et du stockage de renseignements protégés/classifiés par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC). Le bureau de l'agent de sécurité du ministère (ASM) valide ensuite la certification et en avise le coordonnateur de la sécurité de la TI.

1.2 Vérification de la conformité aux politiques de sécurité

Le bureau de l'ASM demandera une copie du rapport d'inspection de la sécurité de la TI, des recommandations et des réponses du fournisseur.

La CPPM a l'option d'exiger que l'entrepreneur assiste à une session d'information sur la sécurité ou sur la sécurité de la TI. De plus, la CPPM se réserve le droit d'inspecter les installations de l'entrepreneur à une fréquence établie par la Division de la sûreté, de la sécurité et de la gestion des urgences, dans le but 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 protégés/classifiés.

2. Exigences minimales en matière de sécurité de la TI

2.1 Vérification de la conformité aux politiques en matière de sécurité de la TI

La CPPM se réserve le droit d'inspecter les installations de l'entrepreneur à une fréquence établie par la Division des services technologiques ou la Direction de la sécurité de la technologie de l'information, dans le but de vérifier la conformité des installations aux normes et aux politiques du gouvernement du Canada en ce qui a trait aux exigences en matière de prévention, de détection, de réaction et de reprise précisées dans la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information.

2.2 Stockage et élimination des supports de la TI

Tout le matériel, comme les CD/DVD, les clés USB, les disques durs des postes de travail, les disques durs des serveurs et les disques durs des ordinateurs, ainsi que de tout autre appareil (y compris les photocopieurs, les numériseurs et les ordinateurs de bureau) utilisé pour traiter ou stocker des informations

protégées doit être conservé et correctement nettoyé ou désinfecté d'une manière conforme à la norme ITSG-06 du CSTC : Nettoyage et déclassification des dispositifs de stockage de données électroniques à la fin du contrat final.

Si l'équipement nécessite une maintenance ou un soutien technique ou s'il doit être remplacé, le matériel informatique associé au traitement et au stockage des renseignements protégés ou classifiés ne pourra pas être confié à un fournisseur externe.

1.1 Informatique mobile et télétravail

Conserver tous les renseignements électroniques sur les serveurs de la CPPM au moyen d'un ordinateur portable fourni, avec un accès à l'infrastructure à clés publiques sur le serveur, conformément aux procédures internes de la Commission pour les renseignements jusqu'au niveau Protégé B inclusivement. Tout document classé comme étant secret sera uniquement accessible sur place, dans les bureaux de la CPPM, et ne doit pas être enregistré sur le serveur de la Commission.

Ranger l'ordinateur portable (protégé B) dans un contenant adapté à la nature de l'information (classeur verrouillé) conformément à la politique sur la sécurité de la CPPM.

1.2 Signalement des incidents

Il est extrêmement important d'aviser la CPPM et le spécialiste de la TI d'un incident de sécurité concernant les installations et le matériel utilisé pour traiter et stocker les renseignements sensibles relatifs aux contrats conclus avec la Commission.

L'entrepreneur doit déclarer tout incident de sécurité à l'ASM et au spécialiste de la TI dans les plus brefs délais après sa détection ou son signalement.

ANNEXE D

Contrôles de sécurité de la TI