Annexe "E"

NON CLASSIFIÉ

Document technique sur les exigences en matière de sécurité de la technologie de l'information (TI)

Sécurité de la TI, Service correctionnel du Canada

Contrat : 21201-16-2168248
Date : 12 janvier 2015

Le présent document décrit les exigences en matière de sécurité de la TI applicables au contrat susmentionné. Ces exigences découlent de la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI).

1. Chaque entrepreneur qui demande l'accès à des renseignements PROTÉGÉS doit détenir une COTE DE FIABILITÉ valide, octroyée par la Direction de la sécurité industrielle canadienne (DSIC) de Travaux publics et Services gouvernementaux Canada (TPSGC).

2. L'entrepreneur ne doit pas donner accès aux renseignements PROTÉGÉS à ses agents et ses sous-traitants, à des bénévoles, à des délinquants ou à d'autres parties, à moins que ces personnes aient été autorisées par la DSIC, qu'elles détiennent une COTE DE FIABILITÉ valide et qu'elles aient un besoin légitime de connaître les renseignements fournis par le système.

3. L'entrepreneur doit s'assurer que tous ses employés qui prennent part à l'exécution du contrat connaissent parfaitement leurs obligations en matière de sécurité relativement au traitement des renseignements PROTÉGÉS.

4. Tout ordinateur servant au stockage ou au traitement de renseignements PROTÉGÉS doit se trouver dans un espace conforme qui respecte les exigences d'une zone de travail conforme à la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor.

5. Si les renseignements PROTÉGÉS sont stockés ou traités sur un support de stockage amovible, comme une clé USB, ces renseignements doivent être protégés à l'aide d'un mot de passe robuste et chiffrés à l'aide d'un produit conforme aux normes de chiffrement du gouvernement du Canada (GC) telles qu'elles sont définies dans l'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 GC.

6. Lorsqu'il ne les utilise pas, l'entrepreneur doit mettre en lieu sûr tous les supports de stockage amovibles dans un coffre de sécurité conforme aux normes de sécurité du GC dans une zone de travail.

7. 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.

8. Si les renseignements PROTÉGÉS sont envoyés par courriel ou tout autre échange électronique, ils doivent être chiffrés à l'aide d'un produit ou d'un service conforme aux normes de chiffrement du GC, telles qu'elles sont définies dans l'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 GC.

9. 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.

Document technique sur les exigences en matière de sécurité de la technologie de l'information (TI)

Sécurité de la TI, Service correctionnel du Canada

10. Sur tous les ordinateurs utilisés pour le stockage ou le traitement de renseignements PROTÉGÉS, un économiseur d'écran protégé par un mot de passe et réglé aux cinq minutes ou moins doit être activé.

11. Sur tous les ordinateurs utilisés pour le stockage ou le traitement de renseignements PROTÉGÉS, un logiciel antivirus récent doit être installé et mis à jour avec les définitions et les signatures de virus les plus récentes.

12. Sur tous les ordinateurs utilisés pour le stockage ou le traitement de renseignements PROTÉGÉS, le système d'exploitation doit être pris en charge par le fournisseur (c.-à-d. que des correctifs de sécurité récents doivent être encore accessibles et que le produit ne doit pas avoir atteint sa fin de vie utile), et le système d'exploitation le plus récent et les correctifs de sécurité des applications doivent être installés et mis à jour à la version la plus récente.

13. Sur tous les ordinateurs utilisés pour le stockage ou le traitement de renseignements PROTÉGÉS, l'accès à l'information doit être restreint au moyen d'un nom d'utilisateur unique et d'un mot de passe robuste pour chaque utilisateur qui accède à l'information ou utilise l'ordinateur dans lequel se trouve cette information. Les comptes informatiques ne doivent pas être partagés.

14. Les comptes informatiques dotés de privilèges d'administrateur doivent servir exclusivement à l'administration des systèmes et ne doivent pas donner accès à Internet.

15. L'enregistrement d'événements de sécurité doit être activé et ces enregistrements doivent être conservés au moins un mois.

16. Tous les ordinateurs qui servent au stockage ou au traitement de renseignements PROTÉGÉS et qui sont connectés à Internet doivent être munis d'un pare-feu permettant la traduction d'adresse de réseau (NAT), en plus d'être configurés de façon sécuritaire, conformément aux pratiques exemplaires de l'industrie (ex. configuration documentée; enregistrements de sécurité activés, mis à jour et examinés; application d'une règle de refus complet avec exception).

17. L'accès à distance au système d'information, au besoin, doit être configuré de façon sécuritaire, conformément aux pratiques exemplaires de l'industrie (ex. listes de contrôle d'accès, solution d'authentification à deux facteurs, enregistrements de sécurité, aucune tunnellisation fractionnée, client du réseau privé virtuel fourni par l'entrepreneur à l'employé, conformément aux exigences des points 10 à 15 ci-dessus).

18. Il est fortement déconseillé de connecter les ordinateurs utilisés pour traiter des renseignements PROTÉGÉS à des réseaux sans fil ou à des technologies Internet sans fil à large bande et, le cas échéant, l'accès sans fil doit être configuré de façon sécuritaire, conformément aux pratiques exemplaires de l'industrie (ex. routeur configuré avec WPA, communication par identificateur de services [SSID] désactivée, utilisation d'un mot de passe robuste, modification du mot de passe tous les six mois, filtrage MAC).

19. Tous les renseignements PROTÉGÉS dont l'entrepreneur a la garde doivent être stockés dans des ordinateurs et des supports de stockage physiques sous sa garde se trouvant au Canada. Le recours à des services d'infonuagique offerts par un tiers (p. ex., Google Drive, Dropbox) est interdit.

20. À la demande du client, la capacité de supprimer de façon immédiate, sécuritaire et permanente tous les renseignements PROTÉGÉS de n'importe quel ordinateur et support de stockage amovible doit être maintenue.

Document technique sur les exigences en matière de sécurité de la technologie de l'information (TI)

Sécurité de la TI, Service correctionnel du Canada

21. À moins d'obligations contraires prescrites par la loi, tous les dispositifs électroniques utilisés pour le stockage ou le traitement de renseignements PROTÉGÉS, comme les ordinateurs, les imprimantes multifonctions, les photocopieurs, les dispositifs de stockage amovibles et tout autre appareil contenant un disque dur interne, doivent être nettoyés ou éliminés en respectant les procédures de sécurité définies dans la publication ITSG-06 afin de veiller à ce qu'il soit impossible de lire des données PROTÉGÉES résiduelles à partir de ces appareils.

22. Toutes les personnes qui ne détiennent pas de COTE DE FIABILITÉ en vigueur lorsqu'elles procèdent à l'entretien d'un ordinateur utilisé pour traiter ou stocker des renseignements PROTÉGÉS dans les locaux de l'entrepreneur doivent faire l'objet d'une supervision directe afin d'empêcher tout accès non autorisé aux renseignements.

23. S'il faut procéder à l'entretien d'un ordinateur utilisé pour le stockage ou le traitement de renseignements PROTÉGÉS à l'extérieur des locaux de l'entrepreneur, ce dernier devra voir au retrait et à la sécurisation de tout disque dur contenant des renseignements PROTÉGÉS avant que l'ordinateur soit retiré des locaux.

24. S'il a été déterminé que le disque dur d'un ordinateur utilisé pour traiter ou stocker des renseignements PROTÉGÉS n'est plus utilisable, le disque dur doit être remis au chargé de projet aux fins de destruction.

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

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 (i.e. « oui » à la question 11e), les exigences en matière de sécurité de la technologie de l'information suivantes doivent être respectées :

26. Tous les ordinateurs ayant accès au Système de gestion des délinquant(e)s ou à ses applications auxiliaires et au système de courriel de Service correctionnel du Canada doivent :
    a. être configurés avec un système BIOS protégé par un mot de passe.
    b. être configurés avec un système BIOS permettant le démarrage uniquement à partir du lecteur C:\;
    c. avoir leur connectivité sans fil désactivée.

27. L'utilisation des éléments suivants est interdite pour tous les ordinateurs ayant accès au Système de gestion des délinquant(e)s ou à ses applications auxiliaires et au système de courriel de Service correctionnel du Canada :
    a. logiciels de partage de poste à poste permettant de communiquer avec d'autres systèmes;
    b. logiciels de jeu en réseau;
    c. logiciels client-serveur, comme un serveur Web, un serveur proxy, un serveur de fichiers, etc. (l'application Receiver de Citrix est toutefois autorisée);
    d. services de courriel Web (le service Outlook Web Access est toutefois autorisé);
    e. logiciels gratuits et logiciels contributifs; (contactez le service de la sécurité de la TI pour de possibles exceptions)
    f. logiciels de contrôle à distance (le logiciel SimpleHelp est toutefois autorisé);
    g. les logiciels client FTP.