51019-14-6001

Traitement des renseignements protégés
Exigences en matière de sécurité des contrats

Sécurité des TI

Anciens Combattants Canada

1. Introduction

Le présent document énonce les exigences en matière de sécurité des TI qui s'appliquent au contrat 51019-14-6001 actuel conclu avec le Ministère pour le traitement des données protégées jusqu'au niveau « protégé A » (inclusivement). Faute d'une évaluation de la menace et des risques (EMR) officielle et parce que les exigences pour les TI visant l'autorisation de sécurité sont particulières au contrat, ce document vise à présenter les mesures de sécurité minimales nécessaires pour que le traitement de renseignements protégés soit approuvé par le coordonnateur de la sécurité des technologies de l'information (CSTI) du Ministère.

2. Exigences Préalables Obligatoires

2.1 Sécurité de l'information

Les documents en version papier et sur d'autres supports doivent être manipulés et transportés conformément aux directives du gouvernement du Canada. Il faut y indiquer le niveau de classification de sécurité applicable tel qu'indiqué par Anciens Combattants Canada. 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 personnel ne peut transporter les documents relatifs au contrat conclu avec Anciens Combattants Canada à l'intérieur ou à l'extérieur de la zone de sécurité sans l'approbation de l'agent de sécurité du Ministère (ASM) d'Anciens Combattants Canada.

3. Exigences Minimales de sécurité des TI

3.1 Vérification de la conformité aux politiques de sécurité des TI

À une fréquence établie par la section des services de technologie de l'information (TI), Anciens Combattants Canada se réserve le droit d'inspecter les installations de l'entrepreneur afin d'en vérifier la conformité aux normes et aux politiques du gouvernement du Canada concernant les exigences en matière de prévention, de détection, de réponse et de reprise qui sont énoncées dans la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information.*

3.2 Conformité aux politiques du gouvernement du canada

Toutes les activités relatives aux TI doivent être conformes aux exigences décrites dans la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information.* Plus précisément, elles doivent être conformes aux sections 16 à 18 se référant à la prévention, à la réponse et à la reprise.

3.2.1 Prévention

Les mesures de prévention protègent la confidentialité, l'intégrité et la disponibilité de l'information et des biens de TI.

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

L'entrepreneur doit fournir, à la demande du CSTI d'Anciens Combattants Canada, la liste des mesures de protection matérielle mises en œuvre pour protéger les lieux voués au traitement et au stockage des renseignements protégés. Tout l'équipement de traitement des renseignements protégés doit être conservé dans une zone opérationnelle.

Le matériel à l'intérieur de la zone opérationnelle, utilisé pour le traitement des renseignements protégés, doit être autonome ou en réseau « isolé » (c'est-à-dire utilisé pour le traitement de l'information relative au contrat et sans connexion externe à Internet ou à un autre réseau, qu'il soit interne ou non).

Le réseau « isolé » ne doit servir qu'au traitement et au stockage de l'information relative aux contrats avec Anciens Combattants Canada et nulle autre partie.

L'utilisation de la technologie sans fil pour le traitement des renseignements protégés est interdite sans l'approbation expresse écrite de l'ASM d'Anciens Combattants Canada.

3.2.1.2 Stockage, élimination et destruction des supports de TI

Les CD et les DVD, les disques à mémoire flash, les clés USB, les disques durs de poste de travail, l'espace disque de serveur, les bandes de sauvegarde et tous les autres dispositifs servant au traitement ou au stockage de renseignements protégés doivent être identifiés et détaillés par modèle (et par numéro de série pour les disques durs), ou, lorsque c'est impossible, par étiquette. Les appareils ou supports doivent être conservés et stockés ou éliminés correctement par le personnel de la sécurité des TI d'Anciens Combattants Canada en cas de défaillance et de remplacement de l'équipement, ou à la résiliation du contrat.

Sur demande, il faut fournir la liste de l'équipement et des supports utilisés au CSTI d'Anciens Combattants Canada. De plus, seuls l'équipement et les supports identifiés, détaillés et dont il existe une trace documentaire peuvent être employés pour le traitement de renseignements protégés relatifs aux contrats avec Anciens Combattants Canada.

Si l'équipement nécessite une maintenance ou un soutien technique ou s'il doit être remplacé, le matériel informatique associé au traitement et à l'entreposage des renseignements protégés ne peut être confié à un fournisseur externe sans l'approbation du CSTI.

Lorsqu'ils ne sont pas utilisés, les supports doivent être placés dans un endroit approuvé pour l'entreposage des renseignements jusqu'à « Protégé A » inclusivement.

3.2.1.3 Autorisation et contrôle de l'accès

Dans les deux semaines suivant l'attribution du contrat, l'entrepreneur doit fournir au CSTI d'Anciens Combattants Canada la liste de toutes les personnes ayant accès aux renseignements protégés qui doivent être traités pour le Ministère, ainsi que ses politiques et ses procédures visant l'élargissement de cet accès à d'autres personnes ou encore les procédures suivies au moment où une personne se voit retirer cet accès.

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

3.2.1.4 Informatique mobile et télétravail

Puisqu'une configuration en réseau isolé est exigée, il n'est pas nécessaire de fournir des directives concernant l'informatique mobile et le télétravail. Cependant, les renseignements protégés relatifs aux contrats conclus avec Anciens Combattants Canada ne peuvent être traités *que* dans les lieux pour lesquels il y a eu validation par l'ASM d'Anciens Combattants Canada.

3.2.1.5 Sécurité relative aux émanations

La classification de sécurité la plus élevée des renseignements traités dans le cadre du présent contrat est la classification « Protégé A » et, par conséquent, la protection TEMPEST n'est pas exigée pour le moment.

3.2.1.6 Câblage des moyens de télécommunication

Si un réseau isolé est utilisé (plutôt que de l'équipement autonome), il est important de contrôler et de surveiller l'accès au câblage, aux espaces et aux chemins d'accès de télécommunication pour éviter toute connexion, intentionnelle ou non, à un autre réseau.

3.2.1.7 Intégrité des logiciels et mesures de sécurité

L'entrepreneur doit configurer ses systèmes d'exploitation et logiciels d'application servant au traitement de l'information protégée conformément aux pratiques exemplaires en matière de sécurité, comme les trousses d'outils Microsoft Security Compliance Manager pour les serveurs et les clients et la documentation d'Anciens Combattants Canada. Il doit aussi prendre des mesures de protection pour renforcer les serveurs et les postes de travail servant au traitement de l'information protégée et consigner ces mesures dans un document qu'il remettra au CSTI d'Anciens Combattants Canada.

3.2.1.8 Programmes malveillants

Puisque les systèmes traitant les renseignements protégés sont isolés (autonomes ou en réseau isolé), le risque qu'ils soient exposés à des programmes malveillants comme des virus, des chevaux de Troie ou des vers est peu élevé. Cependant, sans l'application des procédures visant

l'implantation de nouveau matériel ou l'utilisation de nouveaux renseignements, ils restent vulnérables. Par conséquent, l'entrepreneur doit installer et utiliser un logiciel antivirus et le mettre à jour régulièrement ainsi que balayer les fichiers électroniques provenant de systèmes externes.

3.2.2 Détection

Il faut être en mesure de détecter les menaces à la sécurité de l'environnement où sont traités les renseignements protégés. Des sources comme des registres de systèmes (observateur d'événements), des logiciels antivirus et d'autres outils de surveillance de systèmes sont utiles même si les systèmes en question sont isolés. Pour protéger l'information de manière appropriée, il faut d'abord être capable de détecter des problèmes comme l'accès non autorisé, les pannes de systèmes ou de services imprévues ou les changements non autorisés apportés au matériel informatique, aux micrologiciels ou aux logiciels. Les mesures de détection mises en œuvre par l'entrepreneur doivent être expliquées par écrit et communiquées au CSTI d'Anciens Combattants Canada.

Réponse et reprise

3.2.2.1 Réponse aux incidents

Selon la Politique sur la sécurité du gouvernement, les ministères doivent « établir des mécanismes pour bien répondre aux incidents reliés aux TI et pour partager rapidement les détails de l'incident avec les ministères responsables ». De la même façon, Anciens Combattants Canada exige que l'entrepreneur ait un processus de réponse aux incidents et une documentation connexe. La documentation relative à la réponse aux incidents doit être fournie, sur demande, au CSTI d'Anciens Combattants Canada.

3.2.2.2 Déclaration d'incidents

Il est extrêmement important d'informer l'ASM et le CSTI d'Anciens Combattants Canada de tout incident de sécurité concernant les installations et le matériel utilisé pour traiter et stocker les renseignements protégés liés aux contrats avec Anciens Combattants Canada.

L'entrepreneur doit déclarer tout incident de sécurité à l'ASM d'Anciens Combattants Canada et au CSTI dans les *deux heures* suivant sa détection ou son signalement.

3.2.2.3 Reprise

La reprise des systèmes et la récupération de l'information sont très importantes dans les environnements de TI. Anciens Combattants Canada exige que l'entrepreneur démontre sa capacité à gérer la reprise des systèmes en fournissant des documents relatifs aux politiques de sauvegarde de systèmes et de serveurs (comme les processus utilisés, les tests de restauration, les périodes de conservation et l'emplacement de supports de sauvegarde). La documentation pertinente doit être fournie, sur demande, au CSTI d'Anciens Combattants Canada.

3.2.2.4 Lieu des travaux

Toutes les activités de saisie, de traitement, d'entreposage, d'accès et de sauvegarde électronique de données doivent être menées au pays, et les données doivent également être entreposées au Canada.