Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

DEMANDE DE PROPOSITIONS

CRTC AF 2017/18 DP # 18-0001

ADMINISTRATEUR DE LA LISTE NATIONALE DES NUMÉROS DE TÉLÉCOMMUNICATION EXCLUS

APPENDICE E

EXIGENCES EN MATIÈRE DE SÉCURITÉ POUR LES TECHNOLOGIES DE L'INFORMATION

Canada

1. Introduction

Ce document traite des exigences de sécurité pour les technologies de l'information (TI) dans le cadre du contrat CRTC AF 2017/18 DP # 18-0100 du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) relativement au traitement de données protégées/classifiées « Protégé A » ou de niveau inférieur. Faute d'une évaluation de la menace et des risques officielle (EMR) 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/classifiés soit approuvé par le coordonnateur en sécurité des TI du ministère :

Nom : [Sera inséré lorsque le contrat sera attribué]
Coordonnateur en sécurité des TI
Conseil de la radiodiffusion et des télécommunications canadiennes
1, Promenade du Portage
Ottawa (Ontario) K1A 0N2
Canada
Tél. : [Sera inséré lorsque le contrat sera attribué]
Courriel : [Sera inséré lorsque le contrat sera attribué]

La sécurité repose sur une plusieurs couches de protections. En d'autres termes, les exigences de sécurité pour les TI (STI), lorsqu'elles sont respectées, permettent de protéger l'information efficacement seulement si d'autres mesures et politiques de sécurité les sous-tendent. Les mesures de protection concernant les lieux, le personnel et la sécurité de l'information conformes à la Politique sur la sécurité du gouvernement (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578) 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.

2. Exigences préalables obligatoires

2.1 Validation de la sécurité des lieux par Travaux publics et Services gouvernementaux Canada

L'application des mesures de sécurité énoncées dans ce 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) du ministère des Travaux publics et des Services gouvernementaux (TPSGC). Le bureau de l'agent de sécurité du ministère (ASM) valide ensuite la certification et en avise le coordonnateur en sécurité des TI.

2.2 Vérification de la conformité aux politiques de sécurité

Le bureau de l'ASM demandera une copie du rapport d'inspection de la sécurité des TI, des recommandations et des réponses du fournisseur lorsque l'inspection sera complétée par le DSIC.

Le CRTC peut demander à l'entrepreneur de participer à une séance de breffage sur la sécurité/STI. De plus, le CRTC se réserve le droit d'inspecter les installations de l'entrepreneur à une fréquence établie selon la Division de la sûreté, de la sécurité et de la gestion des urgences. Ces inspections visent à 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.

3. Exigences minimales de sécurité des TI

3.1 Vérification de la conformité aux politiques de sécurité des TI

Le CRTC se réserve le droit d'inspecter les installations à une fréquence établie par la Division des services technologiques ou la Direction de la sécurité de la technologie de l'information. Ces inspections visent à vérifier la conformité des installations aux normes et aux politiques du gouvernement du Canada concernant les exigences de prévention, de détection, de réaction et de reprise contenues dans la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328).

3.2 Stockage et élimination des supports de TI

À la fin du dernier contrat, 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 les autres dispositifs servant au traitement ou au stockage de renseignements protégés doivent être conservés et adéquatement nettoyés ou éliminés en suivant ce qui est indiqué dans le document Effacement et déclassification des supports d'information électroniques (ITSG-06) du Centre de la sécurité des télécommunications du gouvernement du Canada.

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/classifiés ne peut pas être confié à un fournisseur externe.

3.3 Informatique mobile et télétravail

L'informatique mobile et le télétravail sont interdits. Les ordinateurs portables et tout support amovible, s'ils sont utilisés, qui contiennent de l'information protégée/classifiée ne peuvent pas être retirés de l'emplacement de l'entrepreneur inspecté par la DSIC sans l'autorisation écrite de l'ASM.

3.4 Normes logicielles/de systèmes minimales

Tous les composants logiciels et de systèmes (p. ex. les systèmes d'exploitation, les machines virtuelles, les conteneurs, les hyperviseurs, le matériel serveur, le matériel de mise en réseau, les applications logicielles et de systèmes, les micrologiciels, les pare-feu, etc.) doivent être régulièrement mis à jour afin de corriger les vulnérabilités relatives à la sécurité et d'assurer la disponibilité des systèmes. Le calendrier exact des mises à jour sera déterminé par le CRTC. Le fournisseur doit détenir des contrats de soutien commercial/d'entretien en vigueur à l'heure actuelle pour la liste des composants susmentionnés. Aucun composant de la solution ne doit être rendu à l'étape « fin du soutien » de son cycle de vie pendant toute la durée du contrat. La fin du soutien correspond à une situation où le fournisseur/fabricant de matériel, d'une application logicielle ou d'un système d'exploitation cesse de fournir l'un ou l'autre de ce qui suit : une assistance ou un soutien technique (en ligne, par téléphone ou sur place), des mises à jour des produits, des correctifs de sécurité ou des pièces de rechange pour les produits en question.

De plus, les critères suivants doivent être appliqués :

- aucun accès USB au système associé;
- l'accès à une imprimante doit être restreint à l'impression pour le suivi, la production de rapport et la tenue des dossiers financiers. Des contrôles d'accès doivent être en place pour empêcher l'impression de l'information des consommateurs qui est recueilli par le système. Un registre des impressions doit être tenu et conservé pour un minimum de 30 jours.
- la mise en place d'un test CAPTCHA pour les demandes Web;
- une protection contre un niveau élevé de trafic (lien de 200 Mbps) causé par les attaques de déni de service ou par déni de service distribué;
- schéma de zonage de la solution (segmentation de réseau) à être examiné et approuvé par le CRTC;

- un certificat SSL valide émis par une autorité de certification commerciale afin d'autoriser les communications chiffrées à l'aide du protocole de sécurité de la couche transport (TLS) – TLS/SSL à être examiné et approuvé par le CRTC.

3.5 Déclaration d'incidents

Il est extrêmement important d'aviser l'ASM et le coordonnateur en sécurité des TI du CRTC d'un incident de sécurité concernant les installations et le matériel utilisé pour traiter et stocker les renseignements protégés/classifiés relatifs aux contrats avec le CRTC.

L'entrepreneur doit déclarer tout incident de sécurité à l'ASM et au coordonnateur en sécurité des TI dans les deux heures suivant sa détection ou son signalement.

Nom : [Sera inséré lorsque le contrat sera attribué]
Agent de sécurité du ministère
Conseil de la radiodiffusion et des télécommunications canadiennes
Les Terrasses de la Chaudière, Édifice central
1, Promenade du Portage
Ottawa (Ontario) K1A 0N2
Canada
Tél. : [Sera inséré lorsque le contrat sera attribué]
Courriel : [Sera inséré lorsque le contrat sera attribué]