Ministère de la défense nationale (MDN)

Document sur les critères de connectivité

pour

le contrat W8482-168150

Système d'information (SI) Protégé B

HISTORIQUE DES VERSIONS

VERSION	MODIFICATION DATE	DÉTAILS DES MODIFICATIONS	MODIFIÉ PAR
1.0	2019/10/02	Première ébauche	R. Mongeon
1.1	2019/10/21	Changements proposés par la Direction de la Sécurité (Gestion de l'information) du 18 et 21 oct. 2019 mis en œuvre	R. Mongeon

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Le présent « Document sur les critères de connectivité pour le contrat W8482-168150 SI Protégé B » est fourni conformément aux directives pour établir la section 11.e de la partie C du formulaire 350-103 du Secrétariat du Conseil du Trésor (SCT), lesquelles stipulent :

> « Y aura-t-il un lien électronique entre les systèmes informatiques du fournisseur et ceux du ministère ou de l'agence gouvernementale? Si la réponse est Oui, le fournisseur doit faire approuver ses systèmes informatiques. Le ministère client doit aussi fournir les critères de connectivité qui décrivent en détail les conditions et le niveau de sécurité relativement au lien électronique (habituellement pas plus haut que le niveau PROTÉGÉ B). »

1.2 Le présent document définit les exigences en matière de sécurité de la technologie de l'information (TI) du contrat W8482-168150 du ministère de la Défense nationale (MDN) pour un lien de TI entre le MDN et les systèmes de TI de l'entrepreneur utilisés pour traiter, produire et/ou stocker des renseignements, y compris et jusqu'à concurrence du niveau Protégé B. Le lien de TI devrait être validé et autorisé par la Direction de la sécurité industrielle canadienne (DSIC).

1.3 Dans le présent document, l'expression « renseignements exclusifs » désigne « tous les renseignements de niveau Protégé (A et B) fournis ou créés dans le cadre de ce contrat, quel qu'en soit le type ou la forme, ce qui comprend notamment les renseignements scientifiques, techniques, commerciaux et/ou financiers, qu'ils soient utilisés ou non dans le Programme des marchandises contrôlées de Services publics et Approvisionnement Canada (SPAC) ». Pour obtenir d'autres renseignements sur le Programme des marchandises contrôlées de SPAC, consultez le « Règlement sur les marchandises contrôlées (DORS/2001-32) » à l'adresse https://laws-lois.justice.gc.ca/fra/reglements/DORS-2001-32/ ou envoyez un courriel à dmc-cgd@tpsgc-pwgsc.gc.ca.

1.4 Le présent document doit être lu conjointement avec le « Document sur les exigences en matière de sécurité des TI du contrat W8482-168150 Système d'information (SI) Protégé B », lequel définit les conditions préalables obligatoires, de même que les mesures de sécurité de la TI minimales à appliquer au système d'information (SI) de l'entrepreneur utilisé pour traiter, produire et/ou stocker les renseignements jusqu'au niveau Protégé B inclusivement pour le contrat W8482-168150 du MDN.

1.5 Des renseignements supplémentaires sur la sécurité sont offerts sur Internet par ces organisations : Direction de la sécurité industrielle canadienne (DSIC) de Services publics et Approvisionnement Canada (SPAC), le Centre de la sécurité des télécommunications Canada (CSTC), le Centre canadien pour la cybersécurité et la Gendarmerie royale du Canada (GRC).

1.6 On recommande fortement d'examiner le « Document sur les exigences en matière de sécurité des TI du contrat W8482-168150 SI Protégé B » et l'« Aide-mémoire sur la LVERS » avant de terminer ce document.

2. EXIGENCES MINIMALES DE SÉCURITÉ DES TI

2.1 Critère pour un lien de TI

2.1.1 La section 2 du présent « Document sur les critères de connectivité pour le contrat W8482-168150 SI Protégé B » définit la norme et les conditions du lien de TI, de même que les mesures de sécurité de la TI particulières à lui appliquer, afin de maintenir la confidentialité, l'intégrité et l'accessibilité des renseignements exclusifs.

2.1.2 La portée de ce document consiste à préciser les critères de connectivité minimale nécessaires pour transférer de l'information électronique dans le SI Protégé B du contrat W8482-168150 ou en provenance de ce dernier.

2.1.3 Puisque le contrat W8482-168150 exige le transfert de données en ligne, il est nécessaire qu'un niveau supplémentaire de sécurité de la technologie de l'information soit ajouté pour s'assurer que les données ne sont pas compromises (divulguées, interrompues, modifiées, détruites ou supprimées). Ces critères de connectivité visent à protéger non seulement le SI Protégé B du contrat W8482-168150, mais aussi d'autres SI qui reçoivent des renseignements du SI Protégé B du contrat W8482-168150.

2.2 Description du système de TI

2.2.1 Le SI Protégé B du contrat W8482-168150 doit être utilisé exclusivement pour le MDN et doit être clairement identifié comme étant le SI Protégé B du contrat W8482-168150.

2.2.2 Les données électroniques transférées dans le SI Protégé B du contrat W8482-168150 ne peuvent provenir que d'un SI d'un niveau de sensibilité équivalent ou inférieur. Le lien de TI doit être inspecté et son fonctionnement doit être autorisé par la DSIC.

2.2.3 Il est possible de configurer le SI Protégé B du contrat W8482-168150 comme un RL fermé ou un segment du réseau d'entreprise de l'entrepreneur répondant aux exigences du niveau Protégé B.

2.3 Niveau de sensibilité du lien de TI

2.3.1 Le niveau de sensibilité le plus élevé des renseignements exclusifs du contrat W8482-168150 que l'on peut transférer au moyen de ce lien de TI est Protégé B.

2.4 Méthode de connectivité

2.4.1 Ce paragraphe détaille le type de connectivité entre le SI Protégé B du contrat W8482-168150 de l'entrepreneur et l'infrastructure du MDN (HTTPS, protocole PPP, etc.).

2.4.2 Le type de connectivité entre le SI Protégé B du contrat W8482-168150 de l'entrepreneur et le MDN sera un portail Web HTTPS.

2.5 Type et niveau de chiffrement

2.5.1 Ce paragraphe détaille le type de chiffrement (protocole SSL, AES à 128 bits, dispositifs cryptographiques de type I, etc.) à utiliser pour protéger les renseignements exclusifs du contrat W8482-168150 pendant la transmission au moyen du lien de TI du SI Protégé B du contrat W8482-168150.

2.5.2 Les données électroniques exclusives liées au contrat W8482-168150 doivent être échangées entre le MDN et l'entrepreneur au moyen de liens de TI détenus et contrôlés par l'entrepreneur et sécurisés au minimum selon un protocole de chiffrement AES à 128 bits. Voir « Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111) ».

2.6 Exigences matérielles

2.6.1 Ce paragraphe détaille le type de matériel requis pour faire fonctionner le lien de TI du SI Protégé B du contrat W8482-168150 (passerelle RPV, cryptographie, etc.) au niveau de sensibilité préconisé.

2.6.2 Une connexion client léger fiable doit être établie en utilisant un protocole de chiffrement approuvé pour les communications de type VPN.

2.6.3 Il faut concevoir une connexion client léger fiable pour verrouiller le matériel du ou des appareils à distance et empêcher l'accès aux lecteurs internes ou externes des appareils, aux lecteurs CD-ROM/RW, aux autres ports USB et aux interfaces, à l'exception des composants requis pour permettre un accès sécurisé à un segment distinct du réseau d'entreprise de l'entrepreneur dont les administrateurs ou les agents pourraient avoir besoin pour traiter des renseignements exclusifs.

2.6.4 Tous les renseignements exclusifs doivent être enregistrés sur le segment distinct du réseau d'entreprise de l'entrepreneur, et non sur un dispositif d'extrémité.

2.7 Contrôle de l'accès au lien de TI

2.7.1 Ce paragraphe définit les mesures de contrôle de l'accès à mettre en œuvre pour s'assurer que seul le personnel autorisé a accès au lien de TI du SI Protégé B du contrat W8482-168150.

2.7.2 L'entrepreneur doit présenter au chargé de projet (CP) la liste des personnes ayant accès aux renseignements exclusifs.

2.7.3 La liste « Autorisation et contrôle de l'accès » doit également indiquer le type de compte établi pour chaque utilisateur.

2.7.4 Des comptes d'utilisateur spécifiques doivent être créés pour chaque employé de l'entrepreneur et pour chaque membre du personnel du MDN.

2.7.5 Il faut créer deux types de compte pour le personnel du MDN :

2.7.5.1 les administrateurs du SI Protégé B du contrat W8482-168150 du MDN;

2.7.5.2 les membres autorisés du MDN.

2.7.6 Les administrateurs du SI Protégé B du contrat W8482-168150 du MDN doivent accéder au SI Protégé B du contrat W8482-168150 au moyen d'un lien de TI, tandis que les membres autorisés du MDN (appelés également clients) doivent y accéder à l'aide d'un portail Web pour utilisateurs.

2.7.7 Un compte ne doit jamais être partagé entre plusieurs utilisateurs.

2.7.8 Un compte d'administrateur doit être créé pour chaque administrateur de système.

2.7.9 Si un administrateur doit également se servir du SI Protégé B du contrat W8482-168150 à titre d'utilisateur, il doit détenir un compte d'utilisateur pour le faire.

2.7.10 Aucun compte d'utilisateur générique ne doit être créé pour le SI Protégé B du contrat W8482-168150.

2.7.11 Les comptes d'utilisateur (tous les comptes autres que les comptes d'administrateur) doivent être configurés en fonction de privilèges limités et permettre l'accès aux fichiers et aux dossiers dont les utilisateurs ont besoin pour accomplir leurs tâches.

2.7.12 Mots de passe

2.7.12.1 Les comptes doivent être protégés par un mot de passe.

2.7.12.2 Les mots de passe, qu'il ne faut jamais divulguer, doivent être composés d'au moins huit caractères et d'au moins trois des éléments suivants : une majuscule, une minuscule, un chiffre ou un caractère spécial.

2.7.12.3 Les mots de passe des administrateurs de l'entrepreneur doivent être modifiés à l'ouverture de la première session dans le système et tous les 90 jours après coup.

2.7.12.4 L'option de mémorisation du SE doit être désactivée et les dix dernières modifications du mot de passe doivent être enregistrées.

2.7.12.5 Lorsque le mot de passe par défaut d'un administrateur de système doit être changé, le nouveau mot de passe doit être pris en note et conservé dans une enveloppe scellée.

2.7.12.6 L'enveloppe doit être protégée proportionnellement au niveau de classification des renseignements exclusifs de niveau Protégé B le plus élevé et conservée dans un conteneur verrouillable approuvé.

2.8 Gestion du lien de TI

2.8.1 Ce paragraphe détaille les processus opérationnels, de gestion et de surveillance à appliquer au lien de TI du SI Protégé B du contrat W8482-168150.

2.8.2 Le personnel du MDN doit pouvoir accéder au SI Protégé B du contrat W8482-168150 :

a. au moyen d'un lien de TI utilisé par les administrateurs du SI Protégé B du contrat W8482-168150 du MDN;

b. par un portail Web sécurisé pour les membres autorisés du MDN (également définis comme clients).

2.8.3 Les liens de TI ne sont pas autorisés entre l'entrepreneur et les sous-traitants.

2.8.4 Le transfert de données électroniques doit être contrôlé par l'entrepreneur à l'aide de journaux actifs du SE consultés au minimum sur une base mensuelle. L'examen doit porter sur ce qui suit, sans toutefois s'y limiter : tentatives d'ouverture de session échouées, activité de commande en ligne, fonctionnement inhabituel et erreurs de système.

2.9 Lien de TI et PON

2.9.1 Le PON pour le SI Protégé B du contrat W8482-168150 (cité dans le « Document sur les exigences en matière de sécurité des TI du contrat W8482-168150 SI Protégé B) doit inclure les procédures et les détails sur la configuration de tous les aspects pertinents du lien de TI du

contrat W8482-168150 SI Protégé B mentionné dans le « *Document sur les critères de connectivité du contrat W8482-168150 SI Protégé B* ».