Ministère de la Défense nationale (MDN)

Exigences relatives à la sécurité de la technologie de l'information

Transfert de données

pour le

contrat W8482-168150

HISTORIQUE DES VERSIONS

Série	Date Publication	Version	Modificatifs Détails
1	Mai 2018	1.0	Première ébauche

1. INTRODUCTION

1.1 Le présent document décrit les exigences relatives à la sécurité des technologies de l'information (TI) liées au contrat W8482-168150 du Ministère de la Défense nationale visant le transfert de renseignements électroniques entre le système d'information (défini aux présentes comme le SI W8482-168150) utilisé pour le traitement, la production et, le cas échéant, le stockage de renseignements contractuels y compris et jusqu'à concurrence du niveau SECRET. Le présent document vise à établir les mesures de protection de sécurité des TI minimums requises pour le transfert de renseignements électroniques à destination et en provenance du SI W8482-168150 afin que le processus soit approuvé par la Direction de la sécurité industrielle canadienne (DSIC) de Services publics et Approvisionnement Canada (SPAC) et par le Coordonnateur de la sécurité de la technologie de l'information (CSTI) du MDN.

1.2 Le contrat W8482-168150 pouvant exiger la saisie de données de sources non approuvées, un niveau de sécurité des TI supplémentaire est nécessaire afin de réduire la possibilité d'infection par un maliciel provenant d'une source non approuvée. Ces étapes supplémentaires visent à protéger non seulement le SI W8482-168150, mais aussi d'autres SI intégrant des renseignements du SI W8482-168150. Le transfert de tous les renseignements contractuels dans le SI W8482-168150 devra s'effectuer depuis un poste de travail isolé.

1.3 Au moment de choisir les mesures de protection et les processus concernant la sécurité des TI, les chargés de projet doivent soigneusement étudier les effets que ces mesures et processus auront sur les coûts, le calendrier et les besoins opérationnels. Les chargés de projet doivent s'efforcer de trouver un compromis raisonnable entre le coût accru des exigences relatives à la sécurité et l'atténuation des risques qui découleraient de l'utilisation des clauses de sécurité. Le D Sécur GI du MDN peut, au besoin, aider les chargés de projet à prendre des décisions.

2. EXIGENCES PRÉALABLES OBLIGATOIRES

2.1 Description

2.1.1 Un poste de travail autonome doté d'un anti-maliciel à jour et approuvé doit être utilisé pour le transfert des données électroniques dans le SI W8482-168150. Les données électroniques transférées dans le SI W8482-168150 ne peuvent provenir que d'un SI d'un niveau de sensibilité équivalent ou inférieur. Le transfert des données électroniques dans le SI W8482-168150 doit être autorisé par écrit par le chargé de projet du MDN.

2.2 Terminologie

2.2.1 La terminologie suivante est employée dans ce module à un moment ou à un autre.

2.2.1.1 Le fichier source est celui qui est transféré d'un SI de niveau de sensibilité équivalent or inférieur au SI W8482-168150.

2.2.1.2 Le système source est le SI de niveau de sensibilité des données équivalent ou inférieur d'où provient le fichier source.

2.2.1.3 Le système cible est le SI de niveau de sensibilité des données équivalent ou inférieur intégrant le fichier source.

2.2.1.4 Le support de transfert source est le support matériel, dans le présent cas une clé de mémoire dédiée, utilisé pour transférer le fichier source du système source au poste de travail isolé.

2.2.1.5 Le support de transfert cible est le support matériel, dans le présent cas une clé de mémoire dédiée, utilisé pour transférer le fichier source du poste de travail isolé au système cible.

2.2.2 Le SI W8482-168150 représente le système cible.

2.3 Description du système technologique

2.3.1 Le poste de travail isolé est constitué d'un ordinateur autonome démuni d'équipement périphérique autre qu'un écran, un clavier et une souris.

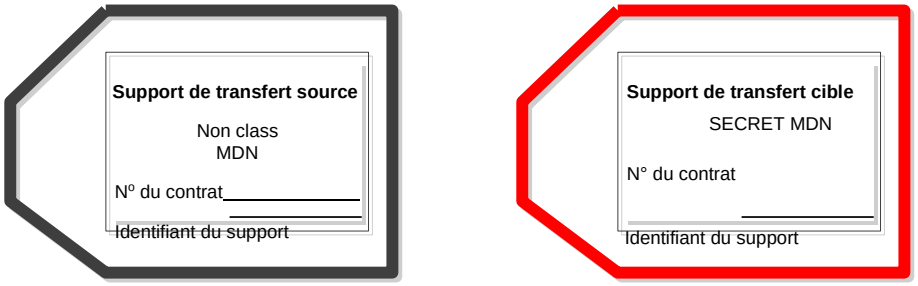
2.3.2 Le poste de travail isolé doit être doté d'un disque dur amovible.

2.3.4 L'équipement du poste de travail isolé doit être étiqueté comme suit.

2.3.4.1 Le poste de travail isolé et le disque dur amovible doivent être étiquetés SECRET.

2.3.4.2 Une grande étiquette aux bordures noires (10 cm par 12 cm) doit être fixée au support de transfert source et indiquée ce qui suit : **Support de transfert source**, niveau de sensibilité des données sources, ministère, numéro du contrat et identifiant unique du support. Voir l'exemple ci-dessous.

2.3.4.3 Une grande étiquette aux bordures rouges (10 cm par 12 cm) doit être fixée au support de transfert cible et indiquée ce qui suit : **Support de transfert cible**, niveau de sensibilité des données sources, ministère, numéro du contrat et identifiant unique du support. Voir l'exemple ci-dessous.



2.3.5 Le poste de travail isolé doit appartenir à l'entrepreneur et être constitué d'un équipement disponible sur le marché, être installé, configuré et fonctionnel avant d'être inspecté par la DSIC.

2.3.6 Le poste de travail isolé doit être installé et être exploité dans la zone de **sécurité** ou dans la zone de **sécurité** temporaire où le SI W8482-168150 est installé, mais il doit être placé à une distance d'au moins un mètre du SI W8482-168150.

2.4 Configuration du système technologique

2.4.1 Le poste de travail isolé doit fonctionner sur un système d'exploitation (SE) pris en charge. Les correctifs de sécurité du SE doivent être mis à jour fréquemment et au moins une fois par mois. Le SE doit être configuré de sorte que les processus, les ports et les fonctions inutiles soient désactivés (c.-à-d. la carte réseau et le microphone). La procédure de mise à jour doit être consignée dans les PUN du poste de travail isolé W8482-168150.

2.4.2 Deux différents antivirus pris en charge doivent être installés sur le poste de travail isolé. Les fichiers de définition des antivirus doivent être mis à jour fréquemment et au moins une fois par mois, et la mise à jour doit être confirmée avant l'analyse anti-malicielle. La procédure de mise à jour doit être consignée dans les PUN du poste de travail isolé W8482-168150.

2.4.3 Un compte doit être créé pour chaque utilisateur et administrateur responsable de l'exploitation et de l'entretien du poste de travail isolé, du SE et des fichiers de définition des antivirus à jour. Si un administrateur doit accéder au poste de travail isolé à titre d'utilisateur, il doit détenir un compte d'utilisateur pour le faire. Aucun compte d'utilisateur générique du poste de travail isolé ne sera autorisé.

2.4.4 Les comptes d'utilisateur doivent être configurés en fonction des privilèges et des accès aux fichiers et aux dossiers que requiert l'utilisateur pour accomplir ses tâches.

2.4.5 L'accès à chaque compte doit être protégé par un mot de passe. Les mots de passe, qui ne doivent jamais être divulgués, sont composés d'au moins huit caractères (une majuscule, une minuscule et un caractère spécial), ils doivent être modifiés à l'ouverture de la première session et tous les 90 jours après cela, et les dix dernières modifications du mot de passe seront enregistrées.

2.4.6 Le mot de passe d'administrateur par défaut doit être modifié, pris en note et conservé dans une enveloppe scellée. L'enveloppe doit être conservée dans un classeur fermé à clé approuvé.

2.4.7 Les fichiers journaux du SE doivent être actifs et examinés au moins une fois par mois. L'examen doit porter sur ce qui suit, sans toutefois s'y limiter : tentatives d'ouverture de session infructueuses, fonctionnement inhabituel et erreurs de système.

2.4.8 Les seules applications permises sur le poste de travail isolé sont le SE et l'antivirus. Les autres applications doivent être supprimées ou désinstallées.

3 PROCÉDURE DE TRANSFERT DES DONNÉES

3.1 Le transfert des données électroniques doit s'effectuer conformément à la procédure suivante.

3.1.1 Le fichier source doit être copié du système source au support de transfert source.

3.1.2 Le support de transfert source doit être connecté au poste de travail isolé et faire l'objet d'une analyse anti-maliciel et antivirus à l'aide des deux applications à cet effet.

3.1.3 Si aucun virus ni maliciel n'est détecté, le fichier source peut être copié sur le disque dur du poste de travail isolé et le support de transfert source peut être retiré du poste de travail isolé.

3.1.4 Puis, le support de transfert cible peut être connecté au poste de travail isolé afin d'y copier le fichier source à partir du poste de travail isolé. Le fichier source peut ensuite être supprimé du disque dur du poste de travail isolé.

3.1.5 Le support de transfert cible doit être retiré du poste de travail isolé puis il peut être connecté au système cible (SIW8482-168150).

3.1.6 Le fichier source épuré peut être copié du support de transfert cible au système cible (SI W8482-168150). Une fois le transfert des données effectué avec succès, le fichier source peut être supprimé du support de transfert cible retiré du système cible

(SI W8482-168150).

3.2 La procédure de transfert des données doit être affichée à proximité du poste de travail isolé.