Ministère de la Défense nationale (MDN)

Document sur les exigences relatives à la sécurité de la technologie de l'information

pour

Le contrat W8482-168150

Système d'information SECRET

HISTORIQUE DES VERSIONS

VERSION	DATE DE MODIFICATION	DÉTAILS DE LA MODIFICATION	MODIFIÉ PAR
1.0	17/09/2019	Ébauche initiale avec le nouveau format. Document original revisé par DIM Secur et envoyer avec la DP selon l'ancien format.	R. Mongeon
1.1	03/10/2019	Deuxième ébauche suite aux commentaire de DIM Secur. Quelques changements additionels ont été ajouté.	R. Mongeon
2	10/10/2019	Version finale approuvée par DIM Secur	R. Mongeon

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Le présent document sur les exigences relatives à la sécurité de la technologie de l'information (TI) pour le contrat W8482-168150 est fourni conformément à l'Instructions de la section 11.d de la partie C du formulaire 350-103 du Secrétariat du Conseil du Trésor (SCT), laquelle stipule :

> « Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et / ou CLASSIFIÉS? Si la réponse est Oui, . . . Le ministère / organisme client devra préciser les exigences en matière de sécurité de la TI relativement à cet achat dans un document technique distinct. . . »

1.2 Le présent document décrit les exigences relatives à la sécurité des TI pour le ministère de la Défense nationale (MDN) visant le traitement, la production et / ou le stockage électronique de l'information jusqu'au SECRET renseignements exclusifs.

1.3 Dans ce document, les « renseignements exclusifs » est définie comme suit:

> « toute information fournie ou générée en vertu du présent contrat, sans tenir compte de la forme ou du type, comprenant, sans toutefois s'y limiter, des informations scientifiques, techniques, commerciales et / ou financières qu'elles soient incluses ou non dans le Programme des marchandises contrôlées de Services publics et Approvisionnements Canada (SPAC). »

D'autres renseignement sur le Programme des marchandises contrôlées de SPAC sont disponibles sur le Règlement sur les marchandises contrôlées (DORS/2001-32) au lieu internet suivant https://laws-lois.justice.gc.ca/fra/reglements/DORS-2001-32/ ou par courriel auprès de dmc-cgd@tpsgc-pwgsc.gc.ca. Dans ce contrat, le contracteur devra avoir accès à de la marchandise contrôlée.

1.4 Le système d'information (SI) utilisé pour traiter, produire et / ou stocker électroniquement des renseignements exclusifs n'est pas requis pour se connecter à l'infrastructure du MDN.

1.5 La sécurité repose sur diverses couches de protection. En d'autres termes, les exigences de sécurité pour les TI, lorsqu'elles sont respectées, permettent de protéger l'information efficacement seulement si d'autres mesures et politiques de sécurité les sous-tendent. Tous travaux contractuels doivent être précédés de l'implémentation de mesures de sécurité physiques, personnelles, procédurales, de l'information et de technologie de l'information.

1.6 D'autres renseignements sur la sécurité sont disponibles sur Internet auprès de la Direction de la sécurité industrielle canadienne (DSIC) de Services publics et Approvisionnement Canada (SPAC), du Centre de la sécurité des télécommunications (CST), du Centre canadien pour la cybersécurité (Cybercentre), et de la Gendarmerie royale du Canada (GRC).

2. CONDITIONS PRÉALABLES OBLIGATOIRES

2.1 Validation de SPAC

2.1.1 L'application des mesures de protection de la sécurité informatique énumérées dans ce document est fondée sur l'exigence obligatoire stipulant que les locaux physiques doivent avoir été inspectés, évalués et autorisés à traiter, à produire et / ou à stocker de l'information SECRET. SPAC ou la DSIC doivent fournir cette validation.

2.1.2 L'entrepreneur doit informer la DSIC et l'OP du MDN de tous les emplacements physiques où on traite, produit et / ou stocke des renseignements exclusifs (p. ex., des bureaux de l'entrepreneur principal et / ou d'un autre entrepreneur, des chantiers de construction, des lieux d'entreposage de secours, des bureaux chez des partenaires et dans des bureaux de sous-traitants et ce, de tous niveaux, etc.). L'entrepreneur doit informer l'OP du MDN et enregistrer officiellement auprès de la DSIC tous les partenaires, tous les niveaux de partenariats et tous les niveaux de sous-traitants qui participent à ce contrat.

2.1.3 Chaque site utilisé pour traiter, produire et / ou stocker électroniquement des renseignements exclusifs de ce contrat doit recevoir une habilitation de sécurité d'installation (HSI) ainsi qu'une vérification des organismes désignés (VOD) ou une autorisation de détenir des renseignements (ADR), selon le cas. De plus, chacun d'entre eux doit être autorisé par la DSIC avant de pouvoir traiter, produire et / ou stocker en format électronique des renseignements exclusifs.

2.1.4 Étant donné qu'on a évalué ce contrat au niveau de classification SECRET, l'entrepreneur doit se conformer aux spécifications de sécurité des émissions (EMSEC) telles que décrites dans le guide de CST/Centre canadien pour la cybersécurité « Conseils relatifs à la sécurité des émissions (EMSEC) (ITSG-11A) », que vous pouvez obtenir auprès de la DSIC ou du OP du MDN.

2.2 Sécurité physique

2.2.1 Le traitement, la production et / ou le stockage des renseignements exclusifs de ce contrat doivent uniquement être effectués dans des installations autorisées par la DSIC. Toutes les données doivent être traitées, produites et / ou stockées de manière sécurisée afin d'empêcher toute visualisation, accès ou manipulation non autorisé.

2.2.2 Conformément au document de la GRC « G1-026 Guide pour l'établissement des zones de sécurité matérielle », le SI (ci-après W8482-168150 SI SECRET) sera installé et opéré dans une zone de sécurité ou dans une zone temporaire de sécurité.

2.2.3 Le traitement, la production et / ou le stockage de renseignements exclusifs de ce contrat effectué à l'extérieur du Canada n'est pas autorisé.

2.2.4 L'informatique mobile / le télétravail/ associé au SI ou aux renseignements exclusifs de ce contrat n'est pas autorisé.

2.3 Sécurité du personnel

2.3.1 Tous les membres du personnel de l'entrepreneur qui ont accès à des renseignements exclusifs de ce contrat doivent :

2.3.1.1 Détenir - à tout le moins - une cote de sécurité du personnel de niveau SECRET valide accordée et dont le suivi est assuré par la DSIC;

2.3.1.2 se voir attribuer les privilèges système selon le critère du moindre privilège. Cela signifie qu'il faut appliquer l'ensemble le plus restrictif de privilèges et le principe du

besoin de savoir (c.-à-d, limiter l'accès à l'information uniquement à ceux qui en ont besoin dans le cadre de leurs fonctions) nécessaires à l'exécution des tâches autorisées;

2.3.2 Aucun visiteur, étranger ou membre du personnel non autorisé ne doit avoir accès aux renseignements exclusifs de ce contrat, au W8482-168150 SI SECRET ou à la zone où on traite, produit et / ou stocke les renseignements exclusifs à moins qu'il possède une cote de sécurité SECRÈTE valide et qu'il soit accompagné par un employé autorisé de l'entrepreneur.

2.3.3 Tous les membres du personnel de l'entrepreneur qui touchent à des renseignements exclusifs de ce contrat doivent recevoir une formation et / ou assister à une séance d'information coordonnée et donnée par l'ASE ou l'ARSE. Cette formation doit, à tout le moins, faire référence au « Manuel de la sécurité industrielle » (MSI) du gouvernement du Canada (GC), à d'autres renseignements sur la sécurité déterminés par l'OP du MDN ainsi qu'aux ordonnances sur la sécurité des TI et aux procédures opérationnelles normalisées (PON) pour le W8482-168150 SI SECRET.

2.4 Sécurité procédurale

2.4.1 L'entrepreneur doit créer des ordonnances de sécurité des systèmes de TI et des PON relatives à l'exploitation ainsi qu'à l'entretien du W8482-168150 SI SECRET. Ces documents doivent, à tout le moins, traiter des éléments suivants.

2.4.1.1 Les rôles et responsabilités (p. ex., de l'ASE, du autorité technique et / ou de l'administrateur du système pour le SI);

2.4.1.2 La gestion des accès pour la zone de sécurité et le SI;

2.4.1.3 L'utilisation acceptable du SI; et

2.4.1.4 Les procédures de gestion des incidents;

2.4.1.5 tout autre sujet identifiées dans le présent document.

2.4.2 Tous les membres du personnel ayant accès au SI doivent lire les ordonnances de sécurité informatique du système et signer un formulaire d'accord d'utilisation connexe, tel que produit et suivi par le l'ASE ou l'ARSE. Tous les changements apportés aux ordonnances, aux PON et / ou au formulaire d'entente de l'utilisateur doivent être transmis à tous les employés qui ont accès au SI.

2.4.3 La gestion et la maintenance du SI doivent être assurées à l'interne par au moins une personne qui possède, à tout le moins, une cote de sécurité SECRÈTE de niveau II valide.

2.4.4 L'entrepreneur doit continuellement surveiller sa situation de sécurité globale, ce qui comprend la sécurité physique, la sécurité du personnel, la sécurité des procédures, la sécurité de l'information et la sécurité des TI. Il doit informer la DSIC et l'OP du MDN de tout problème qui pourrait avoir une incidence sur la sécurité des renseignements exclusifs de ce contrat ou du SI.

2.5 Sécurité de l'information

2.5.1 Tous les documents contenant des renseignements exclusifs de ce contrat doivent porter le niveau de sécurité approprié (des renseignements contenus dans le document) et se voir attribuer un identificateur exclusif afin d'assurer un contrôle et un suivi adéquats.

2.5.2 L'entrepreneur doit protéger la sécurité des enseignements exclusifs «au repos» de ce contrat au moyen de mesures de sécurité physiques et / ou TI.

2.5.2.1 Lorsqu'ils sont laissés sans surveillance, tous les renseignements exclusifs sur papier de ce contrat (p. ex., imprimés papier, etc.) doivent être verrouillés physiquement dans des contenants sécuritaires approuvés.

2.5.2.2 Lorsqu'ils sont sans surveillance, tous les supports informatiques amovibles employés afin de traiter, de produire et / ou de stocker les renseignements exclusifs de ce contrat doivent être verrouillés physiquement dans des conteneurs sécurisés approuvés, ou chiffrés au moyen de la technologie de chiffrement du GC approuvée pour le niveau de sensibilité de ces renseignements exclusifs de ce contrat.

2.5.2.3 Seul le personnel de l'entrepreneur autorisé à avoir accès aux renseignements exclusifs de ce contrat est en mesure de déchiffrer les documents électroniques et / ou d'accéder à la clé ou à la combinaison des conteneurs sécurisés approuvés.

2.5.3 L'échange des renseignements exclusifs de ce contrat entre le MDN et tous les échelons d'entrepreneurs et de sous-traitants peut se faire au moyen d'une copie papier et / ou d'un support informatique amovible. Tous les documents papier et les supports amovibles contenant des renseignements exclusifs de ce contrat doivent être manipulés et transportés ou transmis conformément aux lignes directrices du GC, telles qu'elles sont décrites dans le MSI ou dans le document de la GRC « G1-009 Transport et transmission de renseignements protégés ou classifiés ».

2.5.4 Tous les documents papier et supports informatiques associés à ce contrat doivent être emballés de manière appropriée et transportés ou transmis avec une lettre d'accompagnement ainsi qu'un formulaire de transmission ou un bordereau de circulation qui doit indiquer :

2.5.4.1 le niveau de sensibilité le plus élevé présent dans le support en question;

2.5.4.2 la date de transport ou de transmission;

2.5.4.3 l'identificateur exclusif de chaque document / supports informatiques contenu dans le colis;

2.5.4.4 le nom et le numéro de téléphone de l'expéditeur;

2.5.4.5 l'adresse municipale physique de la destination; et

2.5.4.6 le nom et le numéro de téléphone du destinataire.

2.5.5 L'échange des renseignements exclusifs de ce contrat avec des partenaires, des sous-traitants ou le MDN ne doit pas se faire par l'entremise de liens de TI.

2.5.6 Tous les renseignements exclusifs (p. ex., les documents papier, les supports informatiques, les documents électroniques, etc.) doivent être isolés des autres renseignements contractuels et ministériels d'une manière qui permet de détruire ou d'effacer en intégralité les renseignements exclusifs de ce contrat à la demande de la DSIC ou du OP du MDN, comme l'indique la publication « Nettoyage des supports de TI (ITSP.40.006) » du Centre canadien pour la cybersécurité.

2.5.7 Ultimement, il incombe à l'entrepreneur de s'assurer que toutes les exigences relatives à la sécurité et / ou tous les documents de sécurité pertinents ou connexes relatifs à ce contrat sont fournis aux partenaires de l'entrepreneur et à tous les niveaux de sous-traitants.

3. EXIGENCES MINIMALES RELATIVES À LA SÉCURITÉ DES TI

3.1 Vérification de la conformité à la politique de sécurité des TI

3.1.1 Le MDN se réserve le droit d'inspecter, selon une fréquence et un calendrier à déterminer par le responsable de sécurité de la TI de ce ministère, les installations de chaque entrepreneur participant à ce contrat afin d'assurer la conformité aux exigences de sécurité de la TI énoncées dans la présente ainsi qu'aux normes et politiques du GC en matière de prévention, de détection, d'intervention et de rétablissement.

3.2 Configuration du système de TI

3.2.1 Configuration du système de base : La configuration du système anticipée sera composée d'un ou plusieurs poste(s) de travail autonome(s) TEMPEST (ordinateur ou portatif) avec disques dur amovible pour le (s) poste(s) de travail et l'imprimante local TEMPEST. L'information sera téléchargée à partir du système à l'aide de CD ou DVD, les clés USB ne seront pas autorisés. Un poste de travail isolé autonome doit être utilisé pour balayer ces supports amovibles pour identifier les virus et les anti-maliciels.

3.2.2 Le W8482-168150 SI SECRET doit être configuré comme un réseau local ou un poste de travail autonome sans lien externe.

3.2.3 L'équipement utilisé pour traiter, produire et / ou stocker les renseignements exclusifs doit être composé d'équipement TEMPEST et doit être étiqueté en fonction du niveau de sensibilité de ces renseignements exclusifs de ce contrat (SECRET).

3.2.4 L'équipement de traitement doit comporter des disques durs amovibles. Exemples d'équipement de traitement : postes de travail (p. ex., ordinateurs ou portatifs, tablettes, etc.), serveurs, imprimantes, numériseurs, etc.

3.2.5 Système d'exploitation. Le SI doit fonctionner sur un système d'exploitation (SE) pris en charge, c'est-à-dire que le fournisseur du SE doit créer et fournir les correctifs de sécurité actuels connexes. Il faut installer ceux-ci régulièrement, au moins une fois par mois. Il faut configurer le SE de façon à désactiver les processus, services et ports inutiles. La PON du SI doit indiquer la fréquence et la méthode utilisée pour mettre à jour ces correctifs de sécurité et fournir des détails sur la configuration du SE.

3.2.6 Logiciels antivirus et anti-maliciels. Tous les postes de travail et serveurs (le cas échéant) doivent être dotés d'une logiciel antivirus et anti-maliciel prise en charge et active. Il faut mettre à jour régulièrement les fichiers de définition connexes, au moins une fois par semaine. La PON du SI doit indiquer la fréquence et la méthode employée pour effectuer cette mise à jour ainsi que la configuration de l'application antivirus. Cette configuration doit :

3.2.6.1 n'autoriser que les modifications effectuées par les administrateurs système;

3.2.6.2 analyse automatiquement tous les postes de travail et serveurs du W8481-168150 SI SECRET à la mise sous tension ou à un intervalle défini, au moins une fois par semaine;

3.2.6.3 effectuer l'analyse, à la recherche de code malveillant, de tous les nouveaux fichiers ajoutés aux postes de travail et serveurs du SI.

3.2.7 Logiciels et applications. Seules les applications requises en vertu de ce contrat seront installé sur le SI. Il faut assurer la tenue à jour et la gestion des correctifs d'applications au moyen d'un processus de gestion de configuration défini. La PON du SI doit énumérer chaque application installée et sa version, ainsi que le processus de gestion des correctifs connexe.

3.2.8 Journalisation et vérification. La journalisation du système d'exploitation doit être active et les fichiers journaux doivent être revus au moins une fois par mois par l'administrateur système du W8482-168150 SECRET SI. Cet examen doit porter - entre autres - sur les connexions réussies, les tentatives de connexion infructueuses, les modifications non autorisées du matériel, du micrologiciel et des logiciels du système; le comportement inhabituel de ce dernier; les perturbations imprévues des systèmes et / ou des services; les erreurs du système; etc. Seuls les administrateurs système sont autorisés à modifier ou à supprimer les fichiers journaux et uniquement après en avoir reçu l'autorisation de l'ASE ou de l'ARSE. La PON du SI doit indiquer la fréquence et la méthode utilisée pour effectuer l'examen de ces fichiers.

3.3 Matériel informatique

3.3.1 L'entrepreneur doit tenir à jour une liste de tout l'équipement qui constitue le SI. Cette liste doit fournir, à tout le moins, la description de l'équipement, la marque, le modèle, et la quantité. De plus, l'entrepreneur doit la transmettre sur demande à la DSIC et au OP du MDN.

3.3.2 L'entrepreneur doit informer la DSIC et l'OP du MDN de tout changement majeur apporté au W8482-168150 SI SECRET ou à l'équipement informatique.

3.3.3 L'utilisation de capacités sans fil ou Wi-Fi sur le W8482-168150 SI SECRET est strictement interdite.

3.3.4 L'utilisation de technologie infonuagique pour emmagasiner les renseignements exclusifs de ce contrat est strictement interdite.

3.3.5 L'inter connectivité de tout l'équipement doit :

3.3.5.1 utiliser la fibre optique aux fins de connexion de l'équipement SI;

3.3.5.2 être distinct de tout autre câblage du système;

3.3.5.3 faires l'objet d'un contrôle et d'une surveillance en vue d'empêcher toute connexion accidentelle ou délibérée à toute infrastructure, tout équipement ou tout réseau non autorisé;

3.3.5.4 être installé dans une salle d'interconnexion sécurisé / armoire accessible seulement par l'administrateur W8482-168150 SECRET SI.

3.3.6 Il faut fournir sur demande un diagramme topologique du W8482-168150 SI SECRET à la DSIC et / ou au OP du MDN. Le diagramme doit consister en une conception globale du système.

3.3.7 Les directives de la section « Élimination » présentée ci-dessous doivent être respectées dans le cadre de l'entretien et de l'élimination de tout équipement de TI utilisé pour traiter, produire et / ou stocker les renseignements exclusifs de ce contrat (p. ex., des imprimantes, traceurs, numériseurs, photocopieurs, et / ou des appareils multifonctions, etc.).

3.4 Autorisation et contrôle d'accès

3.4.1 L'entrepreneur doit tenir à jour une liste des personnes autorisées qui ont accès au W8482-168150 SI SECRET. Il faut mettre la liste à jour chaque fois qu'il y a un changement de personnel ou de renseignements sur une personne qui s'y trouve. Elle doit comprendre :

3.4.1.1 le nom de la personne;

3.4.1.2 la cote de sécurité de la personne;

3.4.1.3 le type d'accès (p. ex., utilisateur, utilisateur intensif, administrateur, etc.).

3.4.2 Le W8482-168050 SI SECRET ne doit comporter aucun :

3.4.2.1 compte générique;

3.4.2.2 compte d'invités;

3.4.2.3 compte temporaire;

3.4.2.4 les comptes partagés de toutes sortes.

3.4.3 Il faut créer un compte individuel pour chaque utilisateur et le configurer de façon à n'offrir que des privilèges limités. De plus, il ne doit permettre l'accès qu'aux fichiers et aux dossiers dont l'utilisateur a besoin dans la réalisation de ses tâches.

3.4.4 Il faut créer un compte administrateur individuel pour chaque administrateur système. Si une personne a besoin à la fois d'un accès administrateur et d'un accès utilisateur régulier, elle doit posséder deux comptes distincts sur le W8482-168050 SI SECRET. On ne doit pas employer les comptes administrateur pour réaliser les opérations quotidiennes standard sur le W8482-168050 SI SECRET.

3.4.5 Chaque compte doit être protégé par un mot de passe qui doit avoir un minimum de complexité et qui respecte les exigences suivantes.

3.4.5.1 Il doit contenir au moins huit (8) caractères.

3.4.5.2 Il doit respecter trois des quatre critères suivants :

3.4.5.2.1 au moins une lettre majuscule (A à Z);

3.4.5.2.2 au moins une lettre minuscule (a à z);

3.4.5.2.3 au moins un nombre (0 à 9);

3.4.5.2.4 au moins un caractère spécial (p. ex., !, $, #, %).

3.4.5.3 Sa durée de vie doit être d'au moins un (1) jour, mais pas plus de 90 jours;

3.4.5.4 Il est interdit de réutiliser l'un des dix (10) mots de passe précédents.

3.4.5.5 Le compte se verrouille après quatre (4) tentatives de connexion infructueuses consécutives.

3.4.6 Tout mot de passe utilisé pour accéder au W8482-168050 SI SECRET doit :

3.4.6.1 ne jamais être divulgué à qui que ce soit;

3.4.6.2 être modifié lors de la première connexion;

3.4.6.3 être par la suite modifié tous les 90 jours;

3.4.6.4 être modifié chaque fois qu'on croit qu'il est compromis;

3.4.6.5 ne pas être sauvegardé ou mémorisé par le système d'exploitation ou toute application à laquelle celui-ci accède.

3.4.7 Il faut modifier le mot de passe originel de l'administrateur local sur tous les postes de travail et serveurs formant le SI. On ne doit pas non plus employer ceux par défaut du

fournisseur. Chaque fois qu'on modifie le mot de passe de l'administrateur local, il doit être écrit et placé dans une enveloppe scellée et signée par l'ASE, l'ARSE ou l'administrateur système. Cette enveloppe doit être protégée en fonction du niveau le plus élevé de sensibilité des données traitées sur le W8482-168050 SI SECRET et être verrouillée dans un contenant approuvé.

3.4.8 Tous les éléments réseau (physiques et / ou virtuels) du SI doivent être surveillés et accessibles (p. ex., au moyen d'une liste de contrôle d'accès (LCA), d'Active Directory, etc.) uniquement au personnel autorisé.

3.4.9 La PON du SI doit inclure un processus d'autorisation et de contrôle d'accès décrivant le processus d'ajout, de désactivation et de retrait de l'utilisateur.

3.5 Supports informatiques

3.5.1 Tout au long du contrat, les procédures décrites à la section « Élimination » (présenté ci-dessous) doivent être respecté lors de l'élimination des supports informatiques utilisés pour traiter, produire et / ou stocker les renseignements exclusifs.

3.5.2 Dans les cas de soutien, d'entretien ou de remplacement de l'équipement, **aucun support informatique contenant les renseignements exclusifs de ce contrat** (p. ex., des disques durs internes, des supports amovibles, etc.) ne sera fourni ou mis à la disposition de fournisseur externe, fournisseur de services ou autre personnel non autorisé.

3.5.3 Tous les supports informatiques (p. ex., des disques durs internes, amovibles ou internes, des CD/DVD, etc.) employés pour traiter, produire et / ou stocker les renseignements exclusifs de ce contrat doivent :

3.5.3.1 servir uniquement aux fins de ce contrat;

3.5.3.2 recevoir un identificateur exclusif, aux fins de contrôle et de suivi adéquats;

3.5.3.3 être identifiés et inventoriés selon :

3.5.3.3.1 le type de support (p. ex., CD/DVD, disques durs externes, etc.);

3.5.3.3.2 le niveau de sensibilité de l'information (SECRET);

3.5.3.3.3 la restriction à la divulgation (s'il y a lieu);

3.5.3.3.4 le modèle et le numéro de série (s'il y a lieu).

3.5.3.4 porter des étiquettes indiquant :

3.5.3.4.1 le niveau de sensibilité le plus élevé des données qu'il contient SECRET),

3.5.3.4.2 le ministère (dans ce cas le MDN),

3.5.3.4.3 le numéro du contrat, et

3.5.3.4.4 son identifiant exclusif.

3.5.4 S'il est impossible d'apposer une étiquette directement sur le support, il faut employer d'autres moyens (p. ex., une ficelle, etc.).

3.5.5 Tous les supports informatiques doivent être protégés en fonction du niveau de sensibilité le plus élevé des données qu'ils contiennent (SECRET). Lorsqu'ils ne sont pas utilisé, les supports amovibles, y compris les supports défaillants, ceux possédant un cycle de vie et

ceux d'utilisation à long terme (p. ex., les supports de sauvegarde, etc.), doivent être verrouillés dans un conteneur sécurisé approuvé en fonction du niveau de sensibilité des données qu'ils contiennent (SECRET).

3.5.6 S'il est nécessaire d'interagir avec des sources non fiables dans le cadre de ce présent contrat (p. ex., l'Internet, un autre réseau, des supports informatiques amovibles d'une autre source, etc.), l'entrepreneur doit fournir un poste de travail isolé autonome. Les exigences relatives à la sécurité du transfert des données et les directives connexes pour le poste de travail isolé seront fournies par l'OP du MDN dans un document technique distinct un modèle est disponible sur demande auprès de DIM Secur.

3.5.7 L'emplacement de tous les supports informatiques amovibles doit être suivi et contrôlé à l'aide d'un journal de bord. Ce dernier doit indiquer, à tout le moins :

3.5.7.1 le type de support (p. ex., CD/DVD, etc.);

3.5.7.2 son identificateur exclusif;

3.5.7.3 la date et l'heure de son emprunt;

3.5.7.4 le nom ou les initiales de la personne qui l'a emprunté;

3.5.7.5 la date et l'heure de son retour;

3.5.7.6 le nom ou les initiales de la personne qui l'a retourné.

3.6 Dispositifs de technologie de l'information personnels (DTIPs)

3.6.1 L'entrepreneur doit s'assurer que tous les dispositifs de technologie de l'information personnels (p. ex., des téléphones cellulaires, montres intelligentes, appareils Fitbit, etc.) se trouvent à plus d'un (1) mètre du W8482-168150 SI SECRET.

3.7 Impression et / ou reproduction de documents

3.7.1 L'entrepreneur est :

3.7.1.1 Autorisé à imprimer et / ou à reproduire les renseignements exclusifs de ce contrat dans les locaux de l'entrepreneur;

3.7.1.2 Non autorisé à utiliser des services d'impression et / ou de reproduction externes.

3.7.2 Les imprimantes, traceurs, numériseurs, photocopieurs et / ou appareils multifonctions utilisés pour traiter les renseignements exclusifs de ce contrat ne doivent pas être équipés de disques durs internes.

3.7.3 Toutes les imprimantes, traceurs, numériseurs, photocopieurs et / ou les appareils multifonctions doivent uniquement être connecté au SI. La connexion à d'autres appareils ou réseaux est strictement interdite.

3.7.4 Il est strictement interdit d'employer une connexion commutée à un appareil multifonction qui traite des renseignements exclusifs de ce contrat.

3.7.5 La reproduction de renseignement exclusifs associés à ce présent contrat doit être approuvé par l'OP du MDN. Chaque exemplaire approuvé doit posséder un identificateur exclusif aux fins de contrôle et de suivi adéquats.

3.7.6 Dans le cas où on fait appel à des services d'impression et / ou de reproduction en sous-traitance, le sous-traitant doit se conformer aux exigences établies dans le présent "Document sur les exigences en matière de sécurité des TI du contrat W8482-168150 SI SECRET".

3.8 Récupération

3.8.1 Les renseignements exclusifs de ce contrat doivent être sauvegarder régulièrement, au moins une fois par semaine, à un emplacement distant du système. Si l'entrepreneur ne possède pas un tel emplacement pour protéger les copies de sauvegarde, il est possible de prendre des dispositions à cet égard avec l'OP du MDN. Les copies sauvegardées par un autre partie doivent faire l'objet d'un contrat de sous-traitance. La PON du SI doit inclure des détails sur la fréquence de sauvegarde ainsi que sur la méthodologie et le stockage connexes.

3.8.2 L'entrepreneur doit élaborer et documenter un plan de reprise après sinistre (PRS) pour le W8482-168150 SI SECRET. Ce plan doit comprendre des détails sur la récupération, la restauration, la fréquence des essais et la méthodologie.

3.9 Élimination

3.9.1 L'élimination de tous les supports informatiques utilisés dans le cadre de ce contrat, y compris les supports amovibles et les disques durs internes et externes, doit être autorisée au préalable par l'OP du MDN. De plus, elle doit faire l'objet d'une documentation et d'un suivi. Cela comprend notamment les supports informatiques défectueux, dont le cycle de vie est actif, qui ne sont plus nécessaires, etc. Si les disques durs ne peuvent pas être retirés des périphériques utilisés pour traiter, produire et / ou stocker les renseignements exclusifs (p. ex., tablettes, etc.), les périphériques doivent être renvoyés au OP du MDN.

3.9.2 L'élimination des supports informatiques sur place dans les locaux de l'entrepreneur est autorisée comme l'indique la publication ITSP.40.006 – Nettoyage des supports de TI. Si l'entrepreneur ne dispose pas des moyens d'élimination requis, il peut prendre des dispositions à cet égard avec l'OP du MDN.

3.9.3 L'élimination des supports informatiques doit faire l'objet d'un suivi au moyen d'un certificat de destruction ainsi que d'un formulaire de transit et de réception; l'OP du MDN fournira des modèles pour ces documents. L'entrepreneur doit conserver une copie de tous les documents d'élimination des TI comme preuve que le support informatique a été éliminé de façon appropriée. Il doit les fournir sur demande à la DSIC et au OP du MDN.

3.9.4 À la fin du contrat, tous les renseignements exclusifs du contrat (copies papier et électroniques) doivent être remis au OP du MDN. Cela comprend toutes les copies papier des documents ainsi que tous les supports informatiques utilisés pour traiter, produire et / ou stocker les renseignements exclusifs de ce contrat (p. ex., les disques durs internes (utilisés sur les postes de travail, les ordinateurs portatifs, les serveurs, les photocopieurs, des appareils multifonctions, etc.); les lecteurs de CD/DVD; les cartes SD; les disques durs externes; etc.). Si les disques durs ne peuvent pas être retirés des périphériques utilisés pour traiter, produire et / ou stocker les renseignements exclusifs (p. ex., tablettes, etc.), les périphériques doivent être renvoyés au OP du MDN.

3.9.5 S'il faut procéder à l'entretien et / ou à l'élimination du matériel informatique, on doit appliquer le processus suivant <u>avant</u> de retirer tout matériel informatique utilisé pour traiter, produire et / ou stocker les renseignements exclusifs de ce contrat. Ce processus s'applique à tout équipement de TI contenant des supports informatiques (p. ex., des serveurs, postes de travail, imprimantes, traceurs, numériseurs, appareils multifonctions, etc.).

3.9.5.1 Tout appareil utilisé pour imprimer des renseignements exclusifs de ce contrat doit imprimer au moins 50 copies d'une page entièrement remplie de texte non classifié,

afin d'éliminer toute donnée possible restant sur les tambours, courroies ou autrescomposantes internes du dispositif.

3.9.5.2 Il faut retirer et éliminer tous les dispositifs de mémoire non volatile (disques durs internes, amovibles et externes, etc.) conformément aux directives de la présente section;

3.9.5.3 La mémoire volatile (p. ex., mémoire vive, DRAM, SRAM, etc.) doit être épurée en coupant toute alimentation pendant au moins 24 heures consécutives. L'entrepreneur doit s'assurer qu'il n'y a pas de courant dans la mémoire (p. ex., aucune pile interne ni connexion à un autre appareil). S'il a quelque doute que ce soit concernant le retrait de l'alimentation à la mémoire volatile de l'équipement utilisé pour traiter, produire et / ou stocker des renseignements exclusifs de nature très délicate de ce contrat, l'entrepreneur doit retirer cette mémoire et la faire détruire;

Il faut enlever tout autocollant ou marque de sécurité sur l'appareil en rapport avec ce contrat ou le SI;