Ministère de la Défense nationale (MDN)

Document sur les exigences relatives à la sécurité des technologies de l'information (TI)

pour

le système d'information (SI) PROTÉGÉ B

du contrat W8482-168150

HISTORIQUE DES VERSIONS

VERSION	DATE DE MODIFICATION	DÉTAILS DE LA MODIFICATION	MODIFIÉ PAR
1.0	27/09/2019	Ébauche initiale	R. Mongeon
1.1	21/10/2019	Mise en œuvre des modifications de la Dir Sécur GI, 18 et 21 octobre 2019	R. Mongeon

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Le présent document sur les exigences relatives à la sécurité des TI pour le SI PROTÉGÉ B du contrat W8482-168150 est fourni conformément aux instructions pour remplir l'alinéa 11.d de la partie C du formulaire 350-103 du Secrétariat du Conseil du Trésor (SCT) :

> « 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 oui… Le ministère/organisme client devra préciser les exigences relatives à la 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 du Ministère de la Défense nationale (MDN) pour le traitement, la production et le stockage électroniques des renseignements exclusifs du contrat, jusqu'à concurrence du niveau PROTÉGÉ B, inclusivement.

1.3 Dans le présent document, l'expression « renseignements exclusifs » est définie comme suit : « toute information protégée (A et B) fournie ou produite en vertu du présent contrat, peu importe la forme ou le type, y compris, sans toutefois s'y limiter, des informations scientifiques, techniques, commerciales ou financières, qu'elles soient incluses ou non dans le Programme des marchandises contrôlées de Services publics et Approvisionnement Canada (SPAC) ». Pour obtenir de plus amples renseignements sur le Programme des marchandises contrôlées de SPAC, consulter le *Règlement sur les marchandises contrôlées (DORS/2001-32)* à l'adresse https://laws-lois.justice.gc.ca/fra/reglements/DORS-2001-32/, ou écrire à l'adresse dmc-cgd@tpsgc-pwgsc.gc.ca. Aux fins du présent contrat, l'entrepreneur devra avoir accès à des marchandises contrôlées.

1.4 Dans l'éventualité où le système d'information (SI) utilisé pour traiter, produire ou stocker électroniquement ces renseignements exclusifs est requis pour se connecter électroniquement à l'infrastructure du MDN (on a coché « OUI » à l'alinéa 11.e de la partie C de la Liste de vérification des exigences relatives à la sécurité [LVERS]), l'officier de projet (OP) doit remplir un document distinct sur les « critères de connectivité » des liens informatiques au nom du bureau de gestion de projet du MDN. Le document devra être validé et autorisé par la Direction de la sécurité industrielle canadienne (DSIC).

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. On ne doit réaliser des travaux sous-traités qu'après avoir mis en œuvre des mesures de protection physiques, procédurales, du personnel, de l'information et de la sécurité des TI.

1.6 Des renseignements supplémentaires sur la sécurité sont offerts sur Internet par ces organisations : la DSIC de SPAC, le Centre de la sécurité des télécommunications (CST), le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) et la Gendarmerie royale du Canada (GRC).

2. EXIGENCES PRÉALABLES OBLIGATOIRES

2.1 Validation de SPAC

2.1.1 L'application des mesures de sécurité des TI énumérées dans le présent document est fondée sur l'*exigence* obligatoire selon laquelle les locaux physiques ont été inspectés, évalués et autorisés à traiter, à produire ou à stocker de l'information jusqu'à la catégorie PROTÉGÉ B, inclusivement. 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 ou stocke des renseignements exclusifs (p. ex. bureaux principaux ou secondaires de l'entrepreneur, chantiers de construction, lieux d'entreposage de secours, partenaires et bureaux de sous-traitants de tous niveaux). L'entrepreneur doit informer l'OP du MDN de tous les partenaires et de tous les niveaux de partenariat et de sous-traitants qui participent au contrat et les enregistrer officiellement auprès de la DSIC.

2.1.3 Chaque site utilisé pour traiter, produire ou stocker électroniquement les renseignements exclusifs du présent contrat doit recevoir une attestation de sécurité d'installation ainsi qu'une vérification d'organisation désignée ou une autorisation de détenir des renseignements, selon le cas. De plus, chacun d'entre eux doit aussi être autorisé par la DSIC avant de pouvoir traiter, produire ou stocker électroniquement des renseignements exclusifs.

2.2 Sécurité physique

2.2.1 Le traitement, la production ou le stockage des renseignements exclusifs du présent contrat doivent uniquement être effectués dans des installations autorisées par la DSIC. Toutes les données doivent être traitées, produites et stockées de manière sécuritaire, de façon à prévenir l'accès, la visualisation et la manipulation non autorisés.

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

2.2.3 Le traitement, la production et le stockage des renseignements exclusifs ne doivent pas s'effectuer à l'extérieur du Canada.

2.2.4 L'informatique mobile ou le télétravail associé aux renseignements exclusifs de ce contrat peut être autorisé au besoin. Les appareils distants qui seront utilisés pour l'informatique mobile ou le télétravail doivent être connectés au segment de réseau séparé par une connexion client léger sécurisée utilisant un chiffrement des communications RPV approuvé. Les mesures de protection doivent satisfaire aux exigences de la norme « ITSAP.10.016 – Problèmes de sécurité liés au télétravail » du CST.

2.3 Sécurité du personnel

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

2.3.1.1 détenir, à tout le moins, une cote de sécurité de niveau SECRET valide accordée et suivie 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, au SI PROTÉGÉ B W8482-168150 ou à la zone où on traite, produit ou stocke les renseignements exclusifs, à moins de détenir une cote de sécurité de niveau SECRET valide et d'être accompagné par un employé autorisé de l'entrepreneur.

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

2.4 Sécurité procédurale

2.4.1 L'entrepreneur doit créer des consignes de sécurité du système de TI et des PON relatives à l'exploitation et à l'entretien du SI PROTÉGÉ B W8482-168150. 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 responsable technique ou de l'administrateur du système pour le SI);

2.4.1.2 La gestion de l'accès pour la zone de travail et le SI;

2.4.1.3 L'utilisation acceptable du SI;

2.4.1.4 Les procédures de gestion des incidents;

2.4.1.5 Tout autre sujet indiqué dans le présent document.

2.4.2 Tous les membres du personnel ayant accès au SI doivent lire les consignes de sécurité du système de TI et signer un formulaire d'accord d'utilisation connexe, produit et suivi par le l'ASE ou l'ARSE. Toutes les modifications apportées aux consignes de sécurité du système de TI, aux PON ou au formulaire d'accord d'utilisation doivent être transmises à l'ensemble des 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 de niveau SECRET valide.

2.4.4 L'entrepreneur doit continuellement surveiller sa situation de sécurité globale, ce qui comprend la sécurité physique, procédurale, du personnel, de l'information et 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 ou du SI.

2.5 Sécurité de l'information

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

2.5.2 L'entrepreneur doit protéger la sécurité des renseignements exclusifs statiques au moyen de mesures de sécurité physique ou des TI.

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

2.5.2.2 Lorsqu'on ne les utilise pas, tous les supports informatiques amovibles employés pour traiter, produire ou stocker les renseignements exclusifs doivent être verrouillés physiquement dans des contenants sécurisés approuvés, ou chiffrés au moyen d'une technologie approuvée par le GC et appropriée pour le niveau de confidentialité des renseignements exclusifs.

2.5.2.3 Seul le personnel de l'entrepreneur autorisé à avoir accès aux renseignements exclusifs sera en mesure de déchiffrer les documents électroniques ou d'accéder à la clé ou à la combinaison des contenants sécurisés approuvés.

2.5.3 Lors d'échanges de renseignements exclusifs entre le MDN et les entrepreneurs ou les sous-traitants de tous les niveaux, que ce soit par documents papier ou supports informatiques amovibles, tous ces documents et supports 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*. Lors du transport ou de la transmission, tous les supports électroniques doivent être chiffrés au moyen d'une technologie du GC approuvée pour le niveau de confidentialité de l'information qu'ils contiennent.

2.5.4 Tous les documents papier et supports informatiques 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 classification de sécurité le plus élevé de l'information présentée dans le support;

2.5.4.2 la date de transport ou de transmission;

2.5.4.3 l'identificateur exclusif de chaque document ou support informatique 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;

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 peut se faire par l'entremise de liens informatiques autorisés. Ces liens doivent d'abord être validés, inspectés et autorisés par la DSIC ainsi que reconnus et autorisés par le responsable de la sécurité des TI et l'OP du MDN.

2.5.6 Tous les renseignements exclusifs (p. ex. documents papier, supports informatiques et documents électroniques) doivent être isolés des autres renseignements contractuels et opérationnels d'une manière qui permet de les détruire ou de les effacer immédiatement et en toute sécurité à la demande de la DSIC ou de l'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 En définitive, il incombe à l'entrepreneur de veiller à ce que toutes les exigences relatives à la sécurité et tous les documents de sécurité pertinents ou connexes relatifs au présent contrat soient 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 que déterminera son responsable de la sécurité des TI, les installations de chaque entrepreneur participant au présent contrat afin de vérifier la conformité aux exigences relatives à la sécurité des TI énoncées dans les présentes ainsi qu'aux normes et politiques du GC en matière de prévention, de détection, d'intervention et de récupération.

3.2 Configuration du système de TI

3.2.1 Configuration du système de base : À la base, on prévoit que le système sera un segment du réseau d'entreprise de l'entrepreneur qui répondra aux exigences PROTÉGÉ B.

3.2.2 Le SI PROTÉGÉ B W8482-168150 peut être configuré comme un réseau local fermé ou comme un segment du réseau d'entreprise de l'entrepreneur qui répond aux exigences PROTÉGÉ B.

3.2.3 Le matériel utilisé pour traiter, produire ou stocker les renseignements exclusifs peut être un produit standard et doit être étiqueté en fonction du niveau de confidentialité le plus élevé des renseignements exclusifs qu'il traitera.

3.2.4 Si le SI est configuré comme un segment du réseau d'entreprise de l'entrepreneur, ce dernier doit séparer ses réseaux opérationnels en zones de sécurité des TI et mettre en place des mesures de défense du périmètre et de sécurité des réseaux. Le CST et le Centre canadien pour la cybersécurité fournissent des lignes directrices à ce sujet. Voir les documents *Considérations de conception relatives au positionnement des services dans les zones (ITSG-38)* et *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22)*. Il faut fournir des détails sur la méthodologie d'isolement (c.-à-d. diagramme topologique et autres documents jugés nécessaires) à la DSIC et à l'OP du MDN aux fins d'évaluation. L'entrepreneur doit également mettre en œuvre des mesures de défense du périmètre et de sécurité des réseaux pour le SI afin de gérer la totalité du trafic et de protéger les serveurs accessibles de l'extérieur.

3.2.5 Le matériel de traitement doit être configuré de manière à comporter des disques durs internes. Exemples de matériel de traitement pour ce SI : postes de travail (p. ex. ordinateurs de bureau, portables et tablettes), serveurs, imprimantes et numériseurs.

3.2.6 Système d'exploitation (SE). Le SI doit fonctionner sur un 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. Le SE doit être configuré de façon à désactiver les processus, les services et les ports inutiles. La PON du SI doit définir en détail la configuration du SE, en plus d'indiquer la fréquence et la méthode de mise à jour des correctifs de sécurité du SE.

3.2.7 Logiciels antivirus et antimaliciel. Tous les postes de travail et les serveurs (le cas échéant) doivent être dotés de logiciels antivirus et antimaliciel pris en charge et actifs. Il faut mettre à jour régulièrement les fichiers de définition connexes, au moins une fois par semaine. La PON du SI PROTÉGÉ B W8482-168150 doit préciser la configuration de l'application antivirus et indiquer la fréquence et la méthode employée pour mettre à jour les fichiers de définition de l'antivirus ou de l'antimaliciel. Cette configuration doit :

3.2.7.1 autoriser uniquement les modifications effectuées par les administrateurs système;

3.2.7.2 analyser automatiquement tous les postes de travail et les serveurs du SI PROTÉGÉ B W8482-168150 à la mise sous tension ou à un intervalle défini, au moins une fois par semaine;

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

3.2.8 Logiciels et applications. Seules les applications requises en vertu du présent contrat doivent être installées sur le SI. Les correctifs d'application doivent être tenus à jour et gérés selon un processus de gestion de la configuration défini. La PON du SI doit énumérer chaque application installée et sa version, ainsi que le processus de gestion des correctifs connexe.

3.2.9 Journalisation et audit. La journalisation du SE doit être active et les fichiers journaux doivent être revus au moins une fois par mois par l'administrateur système du SI PROTÉGÉ B W8482-168150. 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 ou des services et les erreurs du système. 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 d'examen de ces fichiers et la méthode à utiliser.

3.3 Matériel informatique

3.3.1 L'entrepreneur doit tenir à jour la liste de toutes les pièces d'équipement constituant le SI. Cette liste doit fournir, à tout le moins, la description du matériel, la marque, le modèle et la quantité. De plus, l'entrepreneur doit la transmettre sur demande à la DSIC et à l'OP du MDN.

3.3.2 L'entrepreneur doit informer la DSIC et l'OP du MDN de tout changement majeur apporté au matériel informatique du SI PROTÉGÉ B W8482-168150.

3.3.3 Il est strictement interdit d'utiliser la technologie sans fil ou les fonctions Wi-Fi sur le SI.

3.3.4 L'utilisation de la technologie infonuagique pour stocker des renseignements exclusifs est strictement interdite.

3.3.5 L'interconnectivité de toutes les pièces d'équipement doit faire l'objet d'un contrôle et d'une surveillance en vue d'empêcher les connexions accidentelles ou délibérées à toute infrastructure ou à tout équipement non autorisé. (On s'attend à ce qu'il s'agisse d'un segment du réseau d'entreprise existant);

3.3.6 Sur demande, un diagramme topologique du SI PROTÉGÉ B W8482-168150 doit être fourni à la DSIC ou à l'OP du MDN. Il doit consister en une conception globale du système et inclure tous les liens informatiques avec d'autres entités ainsi que les connexions à d'autres réseaux ou systèmes, le cas échéant.

3.3.7 Les directives de la section « Élimination » ci-dessous doivent être respectées pour l'entretien et de l'élimination de tout matériel de TI utilisé pour traiter, produire ou stocker des renseignements exclusifs (p. ex. imprimantes, traceurs, numériseurs, photocopieurs et appareils multifonctions).

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 SI. La liste doit être mise 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 les éléments suivants :

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).

3.4.2 Le SI 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 compte partagé de toute sorte.

3.4.3 Un compte doit être créé pour chaque utilisateur et configuré de façon à n'offrir que des privilèges limités. De plus, il doit permettre l'accès uniquement 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 courant, elle doit posséder deux comptes distincts sur le SI. On ne doit pas employer les comptes administrateur pour réaliser les opérations quotidiennes standard.

3.4.5 Chaque compte doit être protégé par un mot de passe qui doit avoir un minimum de complexité et comprendre les éléments suivants :

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 (de A à Z);

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

3.4.5.2.3 au moins un nombre (de 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 SI :

3.4.6.1 ne doit jamais être divulgué à qui que ce soit;

3.4.6.2 doit être modifié lors de la première connexion;

3.4.6.3 doit être par la suite modifié tous les 90 jours;

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

3.4.6.5 ne doit pas être sauvegardé ou mémorisé par le SE ou toute application à laquelle celui-ci accède.

3.4.7 Il faut modifier le mot de passe de l'administrateur local sur tous les postes de travail et les serveurs formant le SI. On ne doit pas employer les mots de passe 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 dont le rabat est signé par l'ASE, l'ARSE ou l'administrateur système. Cette enveloppe doit être protégée en fonction du niveau de confidentialité le plus élevé des renseignements traités par le système et être verrouillée dans un contenant approuvé.

3.4.8 Tous les éléments réseau (physiques ou virtuels) du SI doivent être surveillés et accessibles (p. ex. au moyen de la liste de contrôle d'accès ou d'Active Directory) uniquement par le 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 suppression des comptes utilisateur.

3.5 Supports informatiques

3.5.1 Tout au long du contrat, il faut éliminer tous les supports informatiques utilisés pour traiter, produire ou stocker des renseignements exclusifs conformément aux procédures décrites dans la section « Élimination » du présent document.

3.5.2 Dans les cas de soutien, d'entretien ou de remplacement du matériel, **aucun support informatique contenant des renseignements exclusifs** (p. ex. disques durs internes ou supports informatiques amovibles) ne sera fourni à tout fournisseur externe, fournisseur de services ou autre personnel non autorisé ou mis à sa disposition.

3.5.3 Tous les supports informatiques (p. ex. disques durs internes, amovibles ou externes, CD, DVD et clés USB) employés pour traiter, produire ou stocker des renseignements exclusifs 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 (CD ou DVD, clé USB, etc.),
  - 3.5.3.3.2 le niveau de confidentialité de l'information,
  - 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 confidentialité le plus élevé des données qu'il contient,
  - 3.5.3.4.2 le ministère (dans ce cas-ci, le MDN),
  - 3.5.3.4.3 le numéro du contrat,
  - 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).

3.5.5 Tous les supports informatiques doivent être protégés en fonction du niveau de confidentialité le plus élevé des données qu'ils contiennent. Lorsqu'on ne les utilise pas, tous les supports informatiques amovibles, y compris les supports défaillants, ceux ayant un cycle de vie et ceux pour utilisation à long terme (p. ex. les supports de sauvegarde), doivent être verrouillés dans un contenant sécurisé approuvé en fonction du niveau de confidentialité des données qu'ils contiennent.

3.5.6 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 :

3.5.6.1 le type de support (CD ou DVD, clé USB, etc.);

3.5.6.2 son identificateur exclusif;

3.5.6.3 la date et l'heure de son retrait;

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

3.5.6.5 la date et l'heure de son retour;

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

3.6 Impression ou reproduction de documents

3.6.1 L'entrepreneur est :

3.6.1.1 autorisé à imprimer ou à reproduire tout renseignement exclusif dans ses locaux;

3.6.1.2 non autorisé à utiliser des services d'impression ou de reproduction externes.

3.6.2 Les imprimantes, traceurs, numériseurs, photocopieurs ou appareils multifonctions utilisés pour traiter les renseignements exclusifs ne doivent pas être dotés de disques durs amovibles.

3.6.3 À moins que le SI soit configuré comme un segment du réseau d'entreprise de l'entrepreneur, il faut uniquement connecter les imprimantes, traceurs, numériseurs, photocopieurs ou appareils multifonctions au SI. La connexion à d'autres appareils ou réseaux est strictement interdite.

3.6.4 Il est strictement interdit de brancher une ligne téléphonique à un appareil multifonction qui traite des renseignements exclusifs.

3.6.5 La reproduction de renseignements exclusifs doit d'abord être approuvée par l'OP du MDN.

3.7 Récupération

3.7.1 Il faut sauvegarder les renseignements exclusifs régulièrement (au moins une fois par semaine) et à un emplacement distant. 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 sauvegardes protégées par un tiers doivent faire l'objet d'un contrat de sous-traitance. Les PON du SI du SGC doivent préciser la fréquence, la méthode et le stockage des sauvegardes.

3.7.2 L'entrepreneur doit élaborer et rédiger un plan de reprise après sinistre pour le SI. Ce plan doit comprendre des détails sur la récupération, la restauration, la fréquence des essais et la méthodologie.

3.8 Élimination

3.8.1 L'élimination de tous les supports informatiques utilisés dans le cadre du contrat, y compris les supports amovibles et les disques durs internes et externes, doit être autorisée au préalable par l'OP du MDN, être consignée et faire l'objet d'un suivi. Ces supports comprennent notamment les supports informatiques défectueux, dont le cycle de vie est actif et qui ne sont plus nécessaires. Si les disques durs ne peuvent pas être retirés des dispositifs utilisés pour traiter, produire ou stocker des renseignements exclusifs (p. ex., tablettes), les dispositifs doivent être retournés à l'OP du MDN.

3.8.2 L'élimination des supports informatiques sur place dans les locaux de l'entrepreneur est autorisée selon les conditions suivantes : seulement avec la permission de l'OP du MDN, l'élimination doit être effectuée conformément à la norme ITSP 40.006 du CST. Si l'entrepreneur ne dispose pas des moyens d'élimination requis, il peut prendre des dispositions à cet égard avec l'OP du MDN.

3.8.3 L'élimination des supports informatiques doit faire l'objet d'un suivi au moyen d'un certificat de destruction (le cas échéant) ainsi que d'un formulaire de transit et de réception; l'OP du MDN fournira des modèles pour les deux 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 à l'OP du MDN.

3.8.4 À la fin du contrat, tous les renseignements exclusifs (copies papier et électroniques) doivent être remis à l'OP du MDN. Cela comprend toutes les copies papier des documents ainsi que tous les supports informatiques utilisés pour traiter, produire ou stocker ces renseignements (p. ex. disques durs internes utilisés sur les postes de travail, les portables, les serveurs, les photocopieurs et les appareils multifonctions, CD, DVD, clés USB, cartes SD et disques durs externes). Si les disques durs ne peuvent pas être retirés des dispositifs utilisés pour traiter, produire ou stocker des renseignements exclusifs (p. ex. tablettes), les dispositifs doivent être retournés à l'OP du MDN.

3.8.5 S'il faut procéder à l'entretien ou à l'élimination du matériel informatique, on doit appliquer le processus suivant avant de retirer tout matériel informatique utilisé pour traiter, produire ou stocker des renseignements exclusifs. Ce processus s'applique à tout le matériel contenant des supports informatiques (p. ex. serveurs, postes de travail, imprimantes, traceurs, numériseurs, appareils multifonctions) :

3.8.5.1 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.

3.8.5.2 Il faut épurer la mémoire volatile (p. ex. mémoire vive, DRAM ou SRAM) 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).

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