Ministère de la Défense nationale (MDN)

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

pour le

contrat W8482-168150

HISTORIQUE DES VERSIONS

Série	Date Publication	Version	Modificatifs Détails
1	17 avril 2018	1	Première ébauche
1	20 avril 2018	1.1	Ajout de services d'entretien ou d'élimination d'appareils multifonctions (AM) (3.8.4)
1	25 avril 2018	1.2	Ajout de règles de : Connexions des TI (2.5.7) Schéma de topologie (3.3.3) Modification ou suppression de fichiers journaux (3.3.9)
1	26 avril 2018	1.3	Ajout de conseils sur les exigences relatives à la sécurité des TI (1.3)
1	3 mai 2018	1.4	Modification apportée conformément aux commentaires de M. Lamoureux

1. INTRODUCTION

1.1 Le présent document traite des exigences relatives à la sécurité des technologies de l'information (TI) visant le contrat actuel W8482-168150 du Ministère de la Défense nationale (MDN) pour le traitement, la production et, le cas échéant, le stockage d'information à caractère sensible y compris jusqu'à concurrence du niveau SECRET. Les exigences liées aux TI de l'autorisation de sécurité étant particulières au présent contrat, le document vise à établir les mesures de sécurité des TI minimales nécessaires pour que le traitement, la production et, s'il y a lieu, le stockage d'information à caractère sensible soient approuvés par le fondé de pouvoir du MDN.

1.2 La sécurité repose sur diverses mesures de protection. C'est-à-dire que si les exigences de sécurité des TI (SECTI) sont respectées, elles permettent de protéger l'information efficacement seulement si d'autres mesures et politiques de sécurité les sous-tendent. Avant de retenir des services contractuels, en conformité avec la *Politique sur la sécurité du gouvernement* (PSG) ainsi que la politique, la directive et les normes liées à la SECTI, des mesures de protection concernant les lieux, le personnel et la sécurité de l'information doivent avoir été mises en application avant la mise en œuvre de mesures de protection concernant la SECTI.

1.3 Au moment de choisir les mesures de protection, les chargés de projet doivent soigneusement étudier les effets que ces mesures 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. Validation de la sécurité des lieux par Services publics et Approvisionnement Canada

2.1.1 L'application des mesures de sécurité des TI énoncées dans le présent document est fondée sur l'*exigence obligatoire* selon laquelle il faut inspecter, évaluer et autoriser les lieux destinés au traitement, à la production et au stockage de renseignements de niveau SECRET. La validation doit être fournie par la Direction de la sécurité industrielle canadienne (DSIC) de Services publics et Approvisionnement Canada (SPAC).

2.1.2 L'entrepreneur doit informer la DSIC et le chargé de projet du MDN de tous les lieux où des renseignements contractuels seront traités, produits et, le cas échéant, stockés. Cela comprend, sans toutefois s'y limiter, les bureaux principaux et secondaires de l'entrepreneur, le chantier de construction, l'emplacement du stockage de sauvegarde et les bureaux des partenaires et des sous-traitants de l'entrepreneur.

2.1.3 À la validation, la DSIC avisera le chargé de projet du MDN, le chef de la sécurité industrielle du Directeur – Opérations de sécurité de la défense (DOSD) ainsi que la Direction de Sécurité de la gestion de l'information (D Sécur GI) de l'atteinte de cette exigence. Chaque lieu doit avoir obtenu une attestation de sécurité d'installation, une autorisation de détenir des renseignements et une attestation de sécurité des TI de niveau SECRET de la DSIC avant de pouvoir traiter, produire et, le cas échéant, stocker de l'information à caractère sensible, y compris et jusqu'à concurrence du niveau SECRET.

2.1.4 Les liens technologiques (s'il y a lieu) doivent être validés par la DSIC avant d'être utilisés pour le transfert de renseignements contractuels SECRET.

2.2. Sécurité matérielle

2.2.1 Le SI (dont la désignation aux présentes est le SI W8482-168150) doit être installé et exploité dans une zone de sécurité ou dans une zone de sécurité temporaire conformément à la norme de sécurité de la GRC G1-026.

2.2.2 Le traitement, la production et, le cas échéant, le stockage des renseignements contractuels doivent s'effectuer dans l'installation ou dans les installations autorisées par la DSIC.

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

2.2.5 Il est interdit aux termes du présent contrat d'accéder au SI W8482-168150 par informatique mobile ou par télétravail.

2.3. Sécurité du personnel

2.3.1 Tous les employés de l'entrepreneur autorisés à effectuer le traitement, la production ou le stockage de renseignements contractuels SECRET doivent détenir une autorisation de sécurité du personnel de niveau SECRET et leurs fonctions doivent exiger qu'ils accèdent à ces renseignements. L'autorisation de sécurité de niveau SECRET de l'entrepreneur doit être accordée et surveillée par la DSIC.

2.3.2 Tous les employés de l'entrepreneur traitant de l'information à caractère sensible doivent participer à une séance de formation ou d'information coordonnée et animée par l'agent de sécurité d'entreprise (ASE) ou par son remplaçant. Le Manuel de la sécurité industrielle (MSI) et toute autre publication sur la sécurité que le chargé de projet du MDN juge utiles doivent être abordés dans le cadre de la séance.

2.3.3 Aucun ressortissant étranger ne peut être apte à modifier la confidentialité, l'intégrité et la disponibilité des données sans une autorisation de sécurité du personnel de niveau SECRET valide et l'approbation préalable de la section internationale de la DSIC et du chargé de projet du MDN.

2.3.4 L'accès à la zone où le traitement, la production et, le cas échéant, le stockage des renseignements contractuels s'effectuent est interdit aux visiteurs, au personnel ne détenant pas une autorisation de sécurité du personnel de niveau SECRET valide et au personnel n'y étant pas préalablement autorisé, à moins qu'il ne soit accompagné en tout temps par un entrepreneur autorisé.

2.4. Sécurité administrative

2.4.1 L'entrepreneur doit créer des ordonnances de sécurité des TI du système et des procédures d'utilisation normalisées (PUN) précisant les rôles et responsabilités, la gestion de l'accès, l'utilisation acceptable et la gestion des incidents relativement au fonctionnement et à l'entretien du SI W8482-168150.

2.4.2 L'intégralité du personnel ayant accès au SI doit prendre connaissance des ordonnances de sécurité des TI du système et signer un formulaire de consentement d'utilisateur.

2.4.3 Le SI W8482-168150 doit être administré et entretenu à l'interne par des personnes détenant au moins une autorisation de sécurité du personnel de niveau SECRET valide. L'accès à distance au SI W8482-168150 est interdit.

2.4.4 L'entrepreneur doit surveiller continuellement sa situation générale à l'égard de la sécurité, y compris la sécurité du matériel, du personnel, des procédures, de l'information et des TI, et faire part à la DSIC et au chargé de projet du MDN de toute modification pouvant se répercuter sur la sécurité des renseignements contractuels.

2.5. Sécurité de l'information

2.5.1 Les renseignements contractuels doivent être transmis entre le chargé de projet et l'intégrité des sociétés de l'entrepreneur et de ses sous-traitants sur support papier, sur support technologique et, le cas échéant, par un lien technologique approuvé. Les documents sur support papier et sur d'autres supports technologiques doivent être manipulés et transportés conformément aux directives du gouvernement du Canada (GRC G1-009. Norme opérationnelle sur la sécurité matérielle).

2.5.2 Il faut y indiquer le niveau de classification de sécurité applicable et l'identifiant unique sur tous les documents sur support papier et sur d'autres supports afin d'en garantir le contrôle et le suivi positifs.

2.5.3 Tous les documents sur support papier et sur d'autres supports technologiques doivent être emballés de façon appropriée et être transmis avec une lettre de présentation et un formulaire d'envoi ou un bordereau de circulation annoté afin d'indiquer le niveau le plus élevé de désignation ou de classification des pièces jointes, comme le précise la Liste de vérification des exigences relatives à la sécurité des contrats (LVERS), ainsi que la date de transmission, l'identifiant unique, l'expéditeur et le destinataire du document.

2.5.4 Tous les renseignements contractuels doivent être séparés des autres renseignements contractuels et organisationnels afin qu'ils puissent être effacés de manière sécuritaire à la demande de la DSIC ou du chargé de projet du MDN.

2.5.5 Les renseignements contractuels ne doivent pas être stockés sur des supports infonuagiques externes.

2.5.6 Les liens technologiques entre l'environnement du MDN et l'entrepreneur ou entre l'entrepreneur et d'autres échelons au sein de la société de l'entrepreneur et de ses sous-traitants sont interdits, sauf si la DSIC et le chargé de projet du MDN en ont été informés et les ont autorisés. Le lien technologique (s'il y a lieu) doit être inspecté et validé par la DSIC.

2.5.7 Les connexions technologiques entre le SI W8482-168150 et d'autres réseaux ou équipements sont interdites, sauf si la DSIC et le chargé de projet du MDN en ont été informés et les ont autorisés. Une inspection de la sécurité des TI supplémentaire peut être requise afin de valider et d'autoriser la connexion technologique.

2.5.8 Le chiffrement est habituellement utilisé pour protéger les renseignements inactifs (hébergés dans un système local) ou durant la transmission. Aux termes du présent contrat, le chiffrement ne sera pas nécessaire, car des disques durs amovibles seront utilisés (voir le paragraphe 3.3.5), les supports technologiques seront verrouillés lorsqu'ils seront inutilisés (voir le paragraphe 3.5.5) et aucun lien technologique (voir le paragraphe 2.5.6) ne servira à la transmission d'information à caractère sensible.

3. EXIGENCES MINIMALES DE SÉCURITÉ DES TI

3.1. Vérification de la conformité aux politiques de sécurité des TI

3.1.1 Le MDN se réserve le droit d'inspecter les installations de l'entrepreneur, à une fréquence établie par le Coordonnateur de la sécurité de la technologie de l'information (CSTI) du MDN, afin d'en vérifier la conformité aux exigences relatives à la sécurité aux présentes et aux normes et aux politiques du gouvernement du Canada liées aux exigences en matière de prévention, de détection, d'intervention et de reprise décrites dans la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)* du SCT.

3.2. Équipement de TI

3.2.1 La liste de toutes les pièces d'équipement constituant le SI W8482-168150 doit être tenue à jour par l'entrepreneur. La liste de toutes les pièces d'équipement doit contenir, sans toutefois s'y limiter, la description, la quantité, la marque et le modèle. La liste des pièces d'équipement doit être fournie à la demande de la DSIC et du chargé de projet du MDN.

3.2.2 L'entrepreneur doit informer la DSIC et le chargé de projet du MDN de toute modification apportée à l'équipement constituant le SI W8482-168150.

3.3. Configuration du système technologique

3.3.1 L'équipement servant à effectuer le traitement, la production et, le cas échéant, le stockage des renseignements contractuels doit être constitué d'appareils TEMPEST étiquetés proportionnellement au niveau de sensibilité SECRET correspondant aux renseignements contractuels.

3.3.2 Le SI W8482-168150 doit présenter une configuration de réseau local fermé et dénué d'une connexion externe.

3.3.3 Un diagramme de topologie du SI W8482-168150 doit être fourni à la demande de la DSIC et du chargé de projet du MDN. Ce diagramme doit présenter une conception de système de haut niveau et, s'il y a lieu, les liens technologiques à d'autres entités et, le cas échéant, les connexions à d'autres réseaux ou systèmes.

3.3.4 L'interconnectivité de l'équipement doit reposer entièrement sur des câbles de fibre optique se distinguant des autres câbles du système ministériel, doit être contrôlée et surveillée de sorte à empêcher la connexion involontaire ou délibérée à un appareil, un réseau ou une infrastructure non autorisés et doit passer par des circuits séparés.

3.3.5 Les postes de travail et les serveurs doivent être configurés à partir de disques durs amovibles.

3.3.6 Le SI W8482-168150 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 et ports inutiles soient désactivés. Les PUN du SI W8482-168150 doivent indiquer la fréquence et la méthode de mise à jour des correctifs de sécurité du SE et préciser la configuration du SE.

3.3.7 Un antivirus pris en charge doit être installé et fonctionnel sur le SI W8482-168150. Les fichiers de définition de l'antivirus doivent être mis à jour fréquemment et au moins une fois par mois. L'antivirus doit être configuré de manière à ce que le SI W8482-168150 soit automatiquement analysé chaque fois qu'il est mis sous tension ou selon des intervalles établis. Chaque nouveau fichier versé dans le SI W8482-168150 doit faire l'objet d'une analyse antivirus. Les PUN du SI W8482-168150 doivent indiquer la fréquence et la méthode de mise à jour des fichiers de définition ainsi que la configuration de l'antivirus.

3.3.8 Seules les applications requises aux fins du contrat doivent être installées sur le SI W8482-168150. Les correctifs d'application doivent être tenus à jour et gérés selon un processus de gestion de la configuration défini. Les PUN du SI W8482-168150 doivent indiquer chaque application installée et préciser le processus de gestion des correctifs d'application.

3.3.9 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 échouées, modifications non autorisées du matériel, des micrologiciels ou des logiciels, fonctionnement inhabituel du système, interruptions imprévues du système ou des services et erreurs de système. Les administrateurs de système seront les seuls à pouvoir supprimer des fichiers journaux.
Les PUN du SI W8482-168150 doivent indiquer la fréquence et la méthode d'examen des fichiers journaux du SE.

3.3.10 Il est interdit d'utiliser la technologie sans fil sur le SI W8482-168150.

3.4. Autorisation et contrôle de l'accès

3.4.1 L'entrepreneur doit présenter au chargé de projet du MDN la liste des personnes ayant accès aux renseignements contractuels. Cette liste doit indiquer le type de compte établi pour chaque utilisateur.

3.4.2 Un compte doit être créé pour chaque utilisateur. Un compte ne doit jamais être partagé entre plusieurs utilisateurs.

3.4.3 Un compte d'administrateur doit être créé pour chaque administrateur de système. Si un administrateur doit accéder au SI W8482-168150 à titre d'utilisateur, il doit détenir un compte d'utilisateur pour le faire.

3.4.4 Aucun compte d'utilisateur générique ne doit être créé pour le SI W8482-168150.

3.4.5 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.

3.4.5 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 et d'au moins trois des éléments suivants : une majuscule, une minuscule et un caractère spécial. Le mot de passe doit être modifié à l'ouverture de la première session et tous les 90 jours après cela. L'option de mémorisation du SE doit être désactivée et les dix dernières modifications du mot de passe seront enregistrées.

3.4.7 Le mot de passe d'administrateur par défaut doit être modifié. Le nouveau mot de passe doit être pris en note et conservé dans une enveloppe scellée. L'enveloppe doit être protégée proportionnellement au niveau de classification des renseignements contractuels SECRET le plus élevé et conservée dans un classeur fermé à clé de la GRC approuvé.

3.4.8 Les PUN du SI W8482-168150 doivent prévoir un processus d'autorisation et de contrôle d'accès décrivant la méthode d'ajout et de suppression d'utilisateurs.

3.5. Supports de TI

3.5.1 Chaque support technologique, y compris les disques durs externes, utilisé pour le traitement, la production et, le cas échéant, le stockage des renseignements contractuels doit servir uniquement aux fins du contrat.

3.5.2 Chaque support technologique, y compris les disques durs externes, doit être doté d'un identifiant unique afin d'en garantir le contrôle et le suivi positifs.

3.5.3 Chaque support technologique, y compris les disques durs externes, doit être identifié et répertorié au moyen d'une désignation ou d'une classification, d'une restriction de divulgation et d'un numéro de modèle ou de série (s'il y a lieu). La liste complète des supports technologiques, y compris les disques amovibles et externes, doit être tenue à jour par l'entrepreneur. La liste des supports technologiques doit comprendre, sans toutefois s'y limiter, ce qui suit : description (CD ou DVD, clé de mémoire), numéro de série, s'il y a lieu, identifiant unique. La liste des supports technologiques doit être fournie à la DSIC et au chargé de projet du MDN sur demande.

3.5.4 Chaque support technologique, y compris les disques amovibles et externes, doit être étiqueté. L'étiquette doit indiquer le niveau de classification de sensibilité des renseignements SECRET le plus élevé, le numéro de contrat et l'identifiant unique du support

technologique. Si l'étiquette ne peut être apposée directement sur le support technologique (c.-à-d. les clés de mémoire), elle peut y être accrochée à l'aide d'une corde ou d'un autre moyen.

3.5.5 Tous les supports technologiques, y compris les disques durs externes, doivent être protégés proportionnellement au niveau de classification correspondant à la sensibilité des renseignements contractuels. Les supports technologiques inutilisés (y compris les supports défectueux, en fin de vie utile, excédentaires) doivent être placés dans un classeur fermé à clé de la GRC approuvé.

3.5.6 L'emplacement de tous les supports technologiques doit être contrôlé à l'aide d'un registre. Le registre des supports technologiques doit contenir, sans toutefois s'y limiter, ce qui suit : description, identifiant unique, date de retrait et d'intégration du classeur approuvé et initiales de la personne utilisant le support en question.

3.5.7 Si l'équipement requiert un entretien, un soutien technique ou un remplacement, AUCUN SUPPORT TECHNOLOGIQUE contenant des renseignements contractuels ne doit être confié ou être accessible à un fournisseur de services externe.

3.5.8 Pour la durée du contrat, tout support technologique défectueux, en fin de vie utile, excédentaire doit être éliminé conformément à la section Élimination du présent document.

3.6. Impression et reproduction de documents

3.6.1 L'entrepreneur est autorisé à imprimer et à reproduire des documents contractuels à caractère sensible dans ses propres locaux. Les services d'impression et de reproduction doivent être approuvés par la DSIC et par le chargé de projet du MDN.

3.6.2 Les imprimantes, traceurs, numériseurs et appareils multifonctions (AM) utilisés aux fins du SI W8482-168150 ne doivent pas être dotés de disques durs internes. Autant que possible, les imprimantes, traceurs, numériseurs et AM doivent être dotés de disques amovibles.

3.6.3 L'utilisation d'AM est autorisée si l'appareil est connecté uniquement au SI W8482-168150. La connexion à tout autre appareil, réseau ou téléphone est strictement interdite.

3.6.4 Lorsque des documents contrôlés (désignés par le chargé de projet du MDN) sont reproduits, chaque copie du document original doit être assortie d'un identifiant unique afin d'en garantir le contrôle et le suivi positifs.

3.6.5 Si les services d'impression et de reproduction sont impartis, le sous-traitant doit respecter les **exigences relatives à la sécurité de la technologie de l'information** aux présentes.

3.6.6 En ce qui touche l'entretien et l'élimination des imprimantes, traceurs, numériseurs et AM, les instructions fournies dans la section Élimination s'appliquent.

3.7. Rétablissement

3.7.1 Les renseignements contractuels doivent être sauvegardés régulièrement (au moins une fois par semaine) et être conservés dans un autre emplacement. Si l'entrepreneur n'a pas d'emplacement où conserver les sauvegardes, des dispositions doivent être prises auprès du chargé de projet du MDN. Si les sauvegardes sont conservées chez un autre entrepreneur, la DSIC et le chargé de projet du MDN doivent en être informés et ils doivent valider et autoriser l'initiative. Les PUN du SI W8482-168150 doivent préciser la fréquence, la méthode et le stockage des sauvegardes.

3.7.2 L'entrepreneur doit élaborer et étayer par écrit un plan de reprise du système après sinistre. Les PUN du SI W8482-168150 doivent donner des détails sur la reprise, le rétablissement, les essais, la fréquence et la méthode.

3.8. Élimination

3.8.1 L'élimination de tout support technologique défectueux, en fin de vie utile ou excédentaire, y compris les disques durs amovibles et externes, utilisé aux fins du SI W8482-168150 doit être autorisée par le chargé de projet du MDN et étayée par écrit ou suivie. Il est interdit d'éliminer sur place les supports technologiques.

3.8.2 L'élimination des supports technologiques doit être suivie à l'aide d'un certificat de destruction (dont le gabarit sera fourni par le chargé de projet du MDN), d'un bordereau d'acheminement et d'un formulaire de réception (dont le gabarit sera fourni par le chargé de projet du MDN). L'entrepreneur doit conserver une copie de chaque document attestant de l'élimination d'un support technologique et il doit présenter une telle attestation à la DSIC ou au chargé de projet du MDN s'ils en font la demande.

3.8.3 Tous les supports technologiques contenant des renseignements contractuels doivent être remis au chargé de projet du MDN à la fin du contrat.

3.8.4 Le processus suivant doit s'appliquer avant de retirer pour entretien ou pour élimination une imprimante, un traceur, un numériseur ou un appareil multifonctions (AM) utilisés aux fins du SI W8482-168150.

3.8.4.1 Si l'équipement contient un disque dur interne ou externe ou un autre dispositif de mémoire non volatile, celui-ci doit être retiré et éliminé conformément aux indications susmentionnées.

3.8.4.2 Les dispositifs de mémoire volatile (MV, MVD, MVS) doivent être épurés en interrompant toute alimentation pendant 24 heures. Il faut vérifier qu'il n'y a aucune source d'alimentation interne (p. ex., une pile interne).
REMARQUE : en cas de doute concernant l'interruption de l'alimentation interne de la mémoire volatile dans l'équipement hautement sensible en cours de

déclassement, il convient de simplement retirer la mémoire volatile (MV, MVD, MVS).

3.8.4.3 Toutes les étiquettes et les étiquettes de classification doivent être retirées de l'appareil.

3.8.4.4 En ce qui touche les AM servant au traitement de renseignements classifiés, au moins 50 pages sans classification (non blanches) doivent être photocopiées afin d'effacer toutes les données classifiées restantes sur les tambours ou les courroies de l'appareil.