

J85

**Maintien en puissance des groupes de propulsion
(MPGP)**

ANNEXE G

**TRAITEMENT DE L'INFORMATION
SENSIBLE – EXIGENCES RELATIVES À LA
SÉCURITÉ DES TI**

**MINISTÈRE DE LA DÉFENSE
NATIONALE/NOM DE L'ENTREPRENEUR**

Annexe G : Exigences relatives à la sécurité des TI

1. INTRODUCTION

Le présent document traite des exigences relatives à la sécurité des technologies de l'information (TI) dans le cadre du contrat en cours # (à être identifié) entre le Ministère/l'entrepreneur et (nom de l'entreprise) pour le traitement de données sensibles jusqu'au niveau « Protégé A » inclusivement. Faute d'une évaluation de la menace et des risques (EMR) officielle et parce que les exigences pour les TI visant l'autorisation de sécurité sont propres au contrat, ce document vise à présenter les mesures de sécurité minimales requises pour que le traitement d'information sensible soit approuvé par le gestionnaire de la sécurité/officier de sécurité des systèmes d'information (OSSI) du DPEAG(AEC).

La sécurité repose sur diverses protections. 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. Les mesures de protection concernant les lieux, le personnel et la sécurité de l'information conformes à la Politique sur la sécurité du gouvernement et aux normes connexes de sécurité des TI doivent avoir été mises en application *avant* la mise en œuvre d'exigences relatives à la sécurité des TI.

2. EXIGENCES PRÉALABLES OBLIGATOIRES

2.1. Validation de la sécurité des lieux par Services publics et Approvisionnement Canada

L'application des mesures de sécurité énoncées dans ce document est fondée sur *l'exigence obligatoire* selon laquelle la Direction de la sécurité industrielle canadienne (DSIC) de Services publics et Approvisionnement Canada (SPAC) doit avoir inspecté et certifié les lieux en vue du traitement et du stockage de renseignements sensibles. Le bureau de l'agent de sécurité du Ministère valide ensuite la certification et en avise le gestionnaire de la sécurité/officier de sécurité des systèmes d'information.

Un agent régional de la sécurité industrielle (ARSI) de la DSIC inspecte les lieux deux fois par année pour vérifier si la certification accordée par SPAC continue de s'y appliquer.

2.2. Sécurité du personnel

Tous les membres du personnel ayant accès aux données traitées doivent avoir une autorisation de sécurité du gouvernement du Canada valide pour le niveau approprié (selon la nature plus ou moins sensible de l'information) ainsi que le *besoin de savoir*.

Tous les membres du personnel de (*nom de l'entreprise*) ayant accès à de l'information sensible du gouvernement du Canada (ministère de la Défense nationale) doivent suivre un atelier de

Annexe G : Exigences relatives à la sécurité des TI

formation ou d'information coordonné et animé par l'agent de sécurité du ministère (ASM) et le gestionnaire de la sécurité/officier de sécurité des systèmes d'information du MDN.

2.3. Sécurité de l'information

Les documents en version papier et sur d'autres supports doivent être manipulés et transportés conformément aux directives du gouvernement du Canada. Il faut y indiquer le niveau de classification de sécurité applicable tel qu'il a été attribué par le MDN. Les lettres et les formules d'accompagnement ainsi que les bordereaux de circulation doivent être annotés de manière à indiquer le niveau le plus élevé de classification des pièces jointes.

Le transport de renseignements liés au présent contrat à destination ou en provenance des installations physiques doit être conforme au guide G1-009 *Transport et transmission de renseignements protégés ou classifiés* de la Gendarmerie royale du Canada (GRC). Le personnel de (*nom de l'entreprise*) peut seulement transporter des documents liés à un contrat avec le MDN dans ou à l'extérieur de la *zone de sécurité* après avoir obtenu l'approbation de l'ASM du MDN.

2.4. Vérification de la conformité aux politiques de sécurité

Le MDN se réserve le droit d'inspecter les installations de (*nom de l'entreprise*) à une fréquence établie selon la Division de la sûreté, de la sécurité et de la gestion des urgences. Ces inspections visent à vérifier la conformité des installations aux normes et aux politiques du gouvernement du Canada concernant la manipulation, le stockage et le traitement d'information sensible.

3. EXIGENCES MINIMALES DE SÉCURITÉ DES TI

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

Le MDN se réserve le droit d'inspecter les installations de (*nom de l'entreprise et adresse des installations en question – si connues*) à une fréquence établie par la Division des services technologiques ou la Direction de la sécurité de la technologie de l'information. Ces inspections visent à vérifier la conformité des installations aux normes et aux politiques du gouvernement du Canada concernant les exigences de prévention, de détection, d'intervention et de rétablissement contenues dans la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*.

3.2. Conformité aux politiques du gouvernement du Canada

Toutes les opérations liées à la technologie de l'information doivent se dérouler conformément à l'ensemble des exigences énoncées dans la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*. Plus particulièrement, les articles 16 à 18 sur la prévention, la détection, l'intervention et le rétablissement.

Annexe G : Exigences relatives à la sécurité des TI

3.2.1 Prévention

Les mesures de prévention garantissent la confidentialité, l'intégrité ainsi que la disponibilité de l'information et des biens de TI.

3.2.2 Sécurité des lieux visés par les TI

(Nom de l'entreprise) doit fournir au gestionnaire de la sécurité/officier de sécurité des systèmes d'information la liste des mesures concrètes mises en œuvre pour protéger les lieux voués au traitement et au stockage des renseignements sensibles. Tout l'équipement de traitement des renseignements sensibles doit être conservé dans une *zone de sécurité* conformément au guide G1-026 *Guide pour l'établissement des zones de sécurité matérielle* de la GRC.

Le matériel des *zones de sécurité*, utilisé pour le traitement des renseignements sensibles, doit être autonome ou en réseau *isolé* (c'est-à-dire utilisé pour le traitement de l'information relative au contrat et sans connexion externe à Internet ou à un autre réseau, qu'il soit interne ou non); il peut également se trouver sur le réseau organisationnel de (nom de l'entreprise).

Ce réseau isolé ne doit servir qu'au traitement et au stockage de l'information relative aux contrats et aux contrats de sous-traitance avec le MDN.

Il est interdit d'utiliser la technologie sans fil pour le traitement de renseignements sensibles.

3.2.3 Cryptographie, sécurité des réseaux et défense du périmètre

Le stockage électronique de renseignements désignés « Protégé A » ou « Protégé B » associés au contrat doit être fait dans un environnement de TI approuvé par la DSIC.

Lorsqu'ils sont transmis par voie électronique, les renseignements désignés « Protégé A » doivent être chiffrés si une évaluation de la menace et des risques le justifie. Toutefois, les renseignements « Protégé B » doivent toujours être chiffrés.

Dans le cas des renseignements désignés « Protégé B » et de désignation supérieure, (nom de l'entreprise) doit ségréger ses réseaux en zones de sécurité des TI et mettre en place des mesures de défense du périmètre et de sécurité des réseaux. Le Centre de la sécurité des télécommunications Canada (CSTC) a établi les lignes directrices ITSG-38 et ITSG-22 à ce propos. De plus, l'entrepreneur/fournisseur doit appliquer un contrôle strict sur l'accès à la zone protégée où se trouve l'information associée au contrat. Les mesures de défense du périmètre des réseaux (p. ex. les pare-feu ou routeurs) doivent être utilisées pour gérer l'ensemble du trafic et protéger les serveurs accessibles à partir d'Internet. (Nom de l'entreprise) doit se servir de la technologie de chiffrement approuvée du CSTC pour assurer la confidentialité, l'intégrité, l'authentification et la non-répudiation.

Annexe G : Exigences relatives à la sécurité des TI

Le principe du besoin de connaître doit toujours s'appliquer aux renseignements désignés « Protégé A » et « Protégé B », et ces derniers ne doivent être transmis qu'aux destinataires approuvés.

3.2.4 Stockage, élimination et destruction des supports de TI

Les CD et les DVD, les disques à mémoire flash, les clés USB, les disques durs de poste de travail, l'espace disque de serveur, les bandes de sauvegarde et les autres dispositifs servant au traitement ou au stockage de renseignements sensibles doivent être identifiés et détaillés par modèle (et par numéro de série pour les disques durs), ou, lorsque c'est impossible, par étiquette. Ils doivent être conservés et adéquatement rangés ou éliminés par le personnel de sécurité des TI du MDN en cas de défaillance et de remplacement de l'équipement, ou à la résiliation du contrat.

Il faut fournir la liste de l'équipement et des supports utilisés au gestionnaire de la sécurité/officier de sécurité des systèmes d'information. De plus, seuls l'équipement et les supports identifiés, détaillés et dont il existe une trace documentaire peuvent être employés pour le traitement de renseignements sensibles relatifs aux contrats avec le Ministère.

Si l'équipement nécessite une maintenance ou un soutien technique ou s'il doit être remplacé, le matériel informatique associé au traitement et au stockage des renseignements sensibles ne peut pas être confié à un fournisseur externe.

Lorsqu'ils ne sont pas utilisés, les supports doivent être placés dans un contenant approuvé par la GRC pour le rangement des renseignements de niveau « Secret » ou inférieur (voir le guide G1-001 *Guide d'équipement de sécurité*). L'endroit en question doit faire l'objet d'une vérification par la DSIC et d'une validation par le bureau de l'ASM du MDN.

3.2.4.1 Autorisation et contrôle de l'accès

(Nom de l'entreprise) doit fournir au gestionnaire de la sécurité/officier de sécurité des systèmes d'information la liste de toutes les personnes ayant accès aux renseignements sensibles devant être traités pour le Ministère, ainsi que ses politiques et ses procédures en vigueur visant l'élargissement de cet accès à d'autres ou les procédures suivies au moment où une personne se voit retirer cet accès.

Selon le principe du « droit d'accès minimal », (nom de l'entreprise) doit limiter l'accès au minimum nécessaire pour l'accomplissement des tâches.

Annexe G : Exigences relatives à la sécurité des TI

3.2.4.2 Informatique mobile et télétravail

Puisqu'une configuration en réseau isolé est exigée, il n'est pas nécessaire de fournir des directives concernant l'informatique mobile et le télétravail. Cependant, il est important de mentionner que les renseignements sensibles relatifs aux contrats et aux contrats de sous-traitance conclus avec le MDN *ne peuvent être traités* que dans les lieux qui ont été validés par l'ASM du Ministère.

3.2.4.3 Câblage des moyens de télécommunication

Si un réseau local ou le réseau d'entreprise est utilisé (plutôt que de l'équipement autonome), il est important de contrôler et de surveiller l'accès aux câbles, aux espaces et aux chemins d'accès de télécommunications pour éviter toute connexion, intentionnelle ou non, à un autre réseau.

3.2.4.4 Intégrité des logiciels et configuration de sécurité

(Nom de l'entreprise) doit configurer ses systèmes d'exploitation et logiciels d'application servant au traitement de l'information sensible conformément aux pratiques exemplaires en matière de sécurité (comme les trousseaux d'outils Microsoft Security Compliance Manager pour les serveurs et les clients) et à la documentation de la Direction – Gestion du programme d'équipement aérospatial (DPEAG). La DPEAG doit prendre des mesures de protection pour renforcer les serveurs et les postes de travail servant au traitement de l'information sensible et consigner ces mesures dans un document qu'il remettra au gestionnaire de la sécurité/officier de sécurité des systèmes d'information.

3.2.4.5 Programmes malveillants

(Nom de l'entreprise) doit installer et utiliser un logiciel antivirus et le mettre à jour régulièrement ainsi que balayer les fichiers électroniques provenant de systèmes externes.

3.2.5 Détection

Il faut être en mesure de détecter les menaces à la sécurité de l'environnement où sont traités les renseignements sensibles. Des sources comme des journaux (Observateur d'événements), des logiciels antivirus et d'autres outils de surveillance de systèmes sont utiles même si les systèmes en question sont isolés. Pour protéger l'information de manière appropriée, il faut d'abord être capable de détecter des problèmes comme l'accès non autorisé, les pannes de systèmes ou de services imprévues ou les changements non autorisés apportés au matériel informatique, aux micrologiciels ou aux logiciels. Les mécanismes de détection utilisés par (nom de l'entreprise) doivent être documentés et fournis au gestionnaire de la sécurité/officier de sécurité des systèmes d'information.

Annexe G : Exigences relatives à la sécurité des TI

3.2.6 Intervention et rétablissement

3.2.6.1 Intervention en cas d'incident

Selon la Politique sur la sécurité du gouvernement, les ministères doivent mettre en place des mesures permettant de réagir efficacement aux incidents de sécurité et de communiquer rapidement avec les ministères directeurs désignés à ce sujet. De la même façon, le MDN exige que **(nom de l'entreprise)** ait un processus d'intervention en cas d'incident et un document connexe. La documentation relative à la réaction aux incidents doit être fournie au gestionnaire de la sécurité/officier de sécurité des systèmes d'information.

3.2.6.2 Signalement des incidents

Il est extrêmement important d'aviser l'ASM du MDN et le gestionnaire de la sécurité/officier de sécurité des systèmes d'information d'un incident de sécurité concernant les installations et le matériel utilisé pour traiter et stocker les renseignements sensibles relatifs aux contrats et aux contrats de sous-traitance (le cas échéant) avec le Ministère.

(Nom de l'entreprise) doit déclarer tout incident de sécurité à l'ASM du MDN et au gestionnaire de la sécurité/officier de sécurité des systèmes d'information dans les *deux heures* suivant sa détection ou son signalement. La Direction de la sécurité industrielle canadienne (DSIC) doit également être informée d'un tel incident.

3.2.6.3 Rétablissement

Le rétablissement des systèmes et la récupération de l'information sont très importants dans les environnements de TI. Le ministère de la Défense nationale exige que **(nom de l'entreprise)** démontre sa capacité à gérer le rétablissement des systèmes en fournissant des documents relatifs aux politiques de sauvegarde de systèmes et de serveurs (comme les processus utilisés, les tests de restauration, les périodes de rétention et l'emplacement de supports de sauvegarde). Cette documentation doit être transmise au gestionnaire de la sécurité/officier de sécurité des systèmes d'information.