Politique sur la sécurité des technologies de l'information

1. DATE D'ENTRÉE EN VIGUEUR :

La présente politique ministérielle (PM) entre en vigueur le : 2012 -08 - 06

2. CONTEXTE

En réponse à la *Politique sur la sécurité du gouvernement* du Conseil du Trésor (CT), Travaux publics et Services gouvernementaux Canada (TPSGC) a adopté une structure de sécurité répartie pour mettre en œuvre le programme de sécurité du Ministère. C'est dans ce contexte qu'on a attribué la responsabilité du programme de sécurité des technologies de l'information (TI) du Ministère à la Direction générale des services d'infotechnologie (DGSIT). La gestion de ce programme a, quant à elle, été confiée au coordonnateur de la sécurité des TI. La présente *Politique sur la sécurité des technologies de l'information* vient appuyer ce programme.

Cette PM doit être lue en parallèle avec la *Loi fédérale sur la responsabilité*, la PM sur le *Programme de sécurité du Ministère (051)* ainsi que les instruments de politique du CT suivants : la *Politique sur la gestion des technologies de l'information*, la *Politique sur la sécurité du gouvernement,* la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI), le Cadre stratégique pour l'information et la technologie, ainsi que toutes directives et normes connexes.

La présente PM a pour but d'assurer la sécurité des renseignements électroniques de TPSGC, de ses biens de TI et de ses services connexes. Elle indique les mesures à prendre pour garantir : la confidentialité des renseignements pendant leur stockage, leur traitement ou leur transmission; l'intégrité des renseignements et des processus; la disponibilité des renseignements, ainsi que des systèmes et des services connexes. Elle contient également les mesures de protection des biens utilisés pour recueillir, traiter, recevoir, afficher, transmettre, redéfinir, balayer, stocker ou détruire de façon électronique des données, ces mesures faisant partie du champ d'application de la sécurité des TI.

La présente PM permet de s'assurer que tous les intervenants clés interpréteront de la même manière leur rôle, leurs responsabilités et leurs obligations relativement à la sécurité des TI.

Enfin, elle respecte les politiques connexes du Ministère et du CT, y compris la *Politique sur la sécurité du gouvernement*, ainsi que toutes les lois et tous les règlements applicables.

3. ÉNONCÉ DE POLITIQUE

Travaux publics et Services gouvernementaux Canada doit :

1. maintenir, selon les principes de sécurité des technologies de l'information de TPSGC (cf. annexe B), un programme de sécurité des TI visant à protéger les renseignements

électroniques, les biens de TI et les services connexes, et à lui accorder un financement adéquat;

2. gérer efficacement la sécurité des TI en évaluant continuellement les risques ainsi qu'en mettant en place, en appliquant et en tenant à jour des mesures de prévention, de détection, d'intervention et de rétablissement;

3. surveiller et évaluer les activités liées à la sécurité des TI, puis en faire rapport;

4. veiller à ce que la sécurité des TI fasse partie intégrante des programmes, des services et des activités de TPSGC;

5. communiquer à tous les intervenants leur rôle, leurs responsabilités et leurs obligations relativement à la sécurité des TI. Reportez-vous à ce qui suit :

    - Gestion de la sécurité des technologies de l'information (annexe C);
    - Sécurité des applications (annexe D);
    - Sécurité des opérations des technologies de l'information (annexe E);
    - Gestion des incidents de sécurité des technologies de l'information (annexe F).

4. PORTÉE

La présente PM s'applique aux utilisateurs des TI dans les directions générales de TPSGC, ses organismes de service spéciaux (OSS) et dans les régions. Comptent au nombre des utilisateurs, les employés, les bénévoles, les employés des agences de placement temporaire, les étudiants, les entrepreneurs, les consultants et les partenaires commerciaux qui ont été officiellement autorisés à utiliser les TI de TPSGC.

Elle s'applique également à tous les fournisseurs de services en matière de TI de TPSGC, du secteur privé, aux autres ordres de gouvernement et aux entreprises qui traitent les renseignements de nature délicate du gouvernement ou qui utilisent des biens de TI de nature délicate dans le cadre d'initiatives ou de contrats établis ou gérés par TPSGC, sur place ou à l'extérieur, conformément aux modalités des contrats.

5. DÉFINITIONS

Voir l'annexe A.

6. RESPONSABLITÉS ET OBLIGATIONS REDDITIONNELLES

1. Le **sous-ministre (SM)** doit veiller à la création, dans le cadre du programme de sécurité du Ministère, d'un programme de sécurité des TI efficace et adéquatement financé. Les structures de gestion et de gouvernance sur lesquelles repose ce programme ont pour but de protéger les renseignements électroniques et les biens de TI de nature délicate, de même que les services connexes, qui appartiennent à ou sont gérés par TPSGC. Le SM doit également veiller à ce qu'on surveille et évalue ce programme afin de s'assurer qu'il est efficace et qu'il répond toujours aux besoins du Ministère. Dans ses rapports périodiques sur le programme de sécurité du Ministère, le SM informera le CT de l'état du *Programme de sécurité des TI du Ministère* (051).

    Par ailleurs, le SM est chargé de faciliter les moyens de communication continue avec

les utilisateurs des TI en ce qui a trait à leur rôle, à leurs responsabilités et à leurs obligations.

Il doit nommer le coordonnateur de la sécurité des TI du Ministère et le responsable de la sécurité des communications (SECOM).
Nota : À TPSGC, les responsabilités du coordonnateur de la sécurité des TI et du responsable de la SECOM sont conférées au directeur de la Direction de la sécurité de la TI.

2. Le **directeur, Direction de la sécurité ministérielle**, est l'agent de sécurité du Ministère (ASM), chargé du programme de sécurité des TI (cf. *Programme de sécurité du Ministère [051],* section 5).

3. Le **Dirigeant principal de l'information (DPI)**, de la **Direction générale des services d'infotechnologie (DGSIT**), a la responsabilité de ce qui suit :

    1. élaborer et tenir à jour des cadres de sécurité de l'infrastructure et des applications de TI;

    2. s'assurer que les systèmes de TI ont été certifiés et accrédités avant de les approuver pour exploitation;

    3. élaborer et publier des lignes directrices, des procédures et des normes de sécurité relatives à l'infrastructure, aux applications et aux opérations de TI;

    4. mesurer l'efficacité du programme de protection et de certification de l'infrastructure et des applications de TI, et en informer le responsable de la certification;

    5. sensibiliser les utilisateurs à la sécurité des TI en ce qui concerne les applications, les opérations et l'infrastructure, et leur donner une formation connexe;

    6. surveiller les menaces informatiques et les utilisations inacceptables des réseaux électroniques et de TI du gouvernement, puis signaler les manquements à la sécurité et les incidents au coordonnateur de la sécurité des TI, ainsi qu'au ministère de la Sécurité publique Canada;

    7. déterminer ce qu'il faut faire en cas de contournement d'une mesure de protection;

    8. mettre en œuvre et gérer un processus de saisie et de traitement des données numériques à l'appui des enquêtes et des analyses postérieures aux incidents;

    9. s'assurer que les incidents et les failles de sécurité des TI soient réglés dans les plus brefs délais.

4. Le **coordonnateur de la sécurité des TI** a la responsabilité de ce qui suit :

    1. créer et gérer le programme de sécurité des TI dans le cadre du *Programme de sécurité du Ministère (051)* coordonné;

    2. endosser toutes les PM qui ont une incidence sur la sécurité des TI;

3. veiller à ce que soient vérifiées les sections liées à la sécurité des TI dans la demande de propositions et dans toute autre documentation sur la passation de marchés préparés par TPSGC pour TPSGC, y compris les listes de vérification des exigences relatives à la sécurité (LVERS);

4. endosser tous les contrats établis pour TPSGC et destinés aux fournisseurs externes de services de sécurité des TI ou de biens de TI;

5. travailler en étroite collaboration avec les gestionnaires de la prestation de programmes et de services afin de :

   - vérifier si leurs besoins en matière de sécurité des TI sont satisfaits,

   - leur donner des conseils sur les mesures de protection,

   - les informer des incidences possibles des nouvelles menaces et des menaces existantes,

   - les informer du risque résiduel d'un programme ou d'un service;

6. vérifier la conformité au programme de sécurité des TI et à la présente PM, et en informer les cadres supérieurs du Ministère;

7. concevoir, mettre en œuvre et promouvoir un programme de sensibilisation à la sécurité des TI;

8. mettre en place un processus efficace de gestion des incidents de sécurité des TI et veiller à ce que tous s'y conforment;

9. servir de principale personne-ressource au Ministère en ce qui a trait à la sécurité des TI;

10. aviser l'ASM (directeur, Direction de la sécurité ministérielle) des problèmes réels ou éventuels liés à la sécurité;

11. veiller à l'établissement de mesures visant à protéger l'information gouvernementale que le Ministère a en sa possession, mesures qui devront être approuvées en vertu du processus de gouvernance de la GI-TI;

12. siéger au Comité de sécurité du Ministère et représenter les intérêts du Ministère auprès des organismes responsables des enjeux de sécurité des TI;

13. diriger le programme de certification et d'accréditation de tous les systèmes et applications de TI du Ministère;

14. assurer l'orientation fonctionnelle et la formation des agents de sécurité des systèmes de l'information (ASSI) du Ministère;

15. réviser la présente PM et en évaluer l'efficacité périodiquement;

16. surveiller et évaluer périodiquement le programme de sécurité des TI afin de s'assurer qu'il est efficace et qu'il répond toujours aux besoins du Ministère;

17. examiner les résultats des vérifications internes et en informer les cadres supérieurs du Ministère et l'ASM.

5. Les **chefs de direction générale** ou **d'organisme**, les **directeurs généraux régionaux** et les **directeurs généraux** ont la responsabilité de ce qui suit :

    1. s'assurer de la nomination des ASSI, des autorités locales d'enregistrements (ALE) et des responsables de la SECOM;

    2. mettre en place et coordonner des mesures de protection des TI au sein de leur organisme, à l'appui du programme de sécurité des TI et conformément à celui-ci;

    3. assurer le respect de la présente PM par les utilisateurs dans leur propre organisme et gérer les conséquences associées à toute atteinte à cette PM, et ce, de façon rapide, juste et décisive;

    4. veiller à l'obtention des fonds nécessaires pour vérifier fréquemment la satisfaction des exigences relatives à la sécurité des TI, et signaler à leur ASSI, dans les plus brefs délais, tout manquement ou anomalie à cet égard.

    5. signaler toute non-conformité à la présente PM au coordonnateur de la sécurité des TI.

6. Le **chef adjoint de la surveillance** du **Bureau de la vérification et de l'évaluation** a la responsabilité de vérifier périodiquement le respect de la présente PM par le Ministère et de transmettre ses conclusions au coordonnateur de la sécurité des TI.

7. Le **responsable de la SECOM du Ministère** a la responsabilité de ce qui suit :

    1. conserver le matériel cryptographique et tenir à jour les dossiers;

    2. élaborer des procédures portant sur la SECOM;

    3. vérifier les pratiques en matière de SECOM et corriger les failles;

    4. signaler à l'ASM les problèmes réels et éventuels liés à la SECOM, et s'assurer que des mesures correctives sont prises;

    5. donner des consignes au personnel au sujet de la manipulation du matériel de SECOM et des mesures de sécurité qui s'y rapportent;

    6. relire les contrats, établis par TPSGC pour TPSGC, pour s'assurer qu'ils comportent les clauses pertinentes à l'égard de la SECOM;

    7. traiter les incidents de sécurité de la SECOM et veiller à ce que des mesures correctives soient prises rapidement pour empêcher qu'ils ne se répètent;

    8. veiller à l'élimination et à la destruction du matériel de SECOM remplacé, conformément aux méthodes et aux procédures actuelles;

    9. nommer les responsables principaux et suppléants de la SECOM qui seront

chargés de l’administration du matériel de SECOM du Ministère;

10. assurer l’orientation fonctionnelle et la formation des responsables de la SECOM du Ministère;

11. surveiller le matériel de SECOM et les procédures appliquées par les responsables de la SECOM à TPSGC;

12. surveiller le matériel de SECOM dans le secteur privé et l’industrie, comme le prévoit le *Programme de la sécurité industrielle (054).*

8. Les **agents de sécurité des systèmes de l’information (ASSI)** ont la responsabilité de :

    1. servir de personnes-ressources et de promouvoir le programme de sécurité des TI dans leur secteur d’activité;

    2. faciliter l’interprétation des politiques sur la sécurité des TI et des pratiques exemplaires dans leur secteur d’activité;

    3. participer à la mise en œuvre d’un programme de sensibilisation à la sécurité des TI;

    4. prendre part au processus de gestion des risques associés aux applications, aux systèmes et aux services de TI;

    5. collaborer avec l’agent de sécurité de l’unité (ASU), le représentant de clients et le bureau régional de sécurité ou d’autres groupes pour que tout le personnel dans l’environnement des TI reçoive les attestations de sécurité appropriées;

    6. s’assurer que l’on tient compte des aspects liés à la sécurité des TI avant d’acheter du matériel de TI;

    7. s’assurer que l’on tient compte des aspects liés à la sécurité des TI lorsque des utilisateurs quittent l’organisation;

    8. veiller à ce que l’accès aux systèmes d’information et aux TI soit adéquatement contrôlé;

    9. s’assurer que l’on tient compte des aspects liés à la sécurité des biens de TI sous leur contrôle;

    10. participer à la certification et à l’accréditation des systèmes conçus pour leur secteur d’activité;

    11. surveiller l’accès aux systèmes d’information; signaler les incidents de sécurité reliés aux TI, les infractions à la sécurité et les problèmes éventuels liés à la sécurité au Bureau de services des TI, en composant le 1-866-995-6030, ainsi qu’au bureau régional de sécurité; veiller à ce que des mesures correctives soient prises rapidement pour empêcher qu’ils ne se répètent.

9. Les **autorités locales d’enregistrement (ALE)** ont la responsabilité d’exécuter les fonctions liées à l’émission des justificatifs d’infrastructure à clés publiques (ICP) pour

le compte de TPSGC pour les services qui ne sont pas disponibles sur le système automatisé ou au besoin, selon les besoins opérationnels.

10. Les **directeurs**, les **gestionnaires** et les **superviseurs** ont la responsabilité de ce qui suit :

    1. s'assurer que le programme de sécurité des TI est appliqué dans leur unité organisationnelle;

    2. veiller au respect des pratiques et des procédures en matière de sécurité des TI;

    3. veiller à ce que les utilisateurs qui relèvent d'eux reçoivent la formation en matière de sécurité des TI;

    4. faire en sorte que la présente PM soit connue et respectée de toutes les personnes qui relèvent de leur responsabilité;

    5. planifier les activités nécessaires liées à la sécurité des TI;

    6. établir des procédures et des mesures de protection destinées aux systèmes de TI locaux dans leur organisme, ainsi qu'à l'information qu'ils contiennent;

    7. voir à ce que des énoncés de la nature délicate, des évaluations de la menace et des risques, ainsi que des plans de mesures d'urgence soient réalisés et tenus à jour pour les systèmes d'applications ou les installations dont ils ont la responsabilité;

    8. s'assurer que toute transgression des politiques et des normes sur la sécurité des TI est immédiatement signalée à leur ASSI;

    9. veiller à ce que les exigences et les clauses pertinentes relatives à la sécurité des TI soient comprises dans les contrats, respectées par les fournisseurs et appliquées pendant toute la durée des contrats;

    10. appliquer les recommandations présentées à la suite des examens de la sécurité des TI et confirmer le règlement des problèmes au coordonnateur de la sécurité des TI;

    11. autoriser toute modification du matériel ou des logiciels de TI au moyen du processus officiel de contrôle des changements;

    12. contrôler la conformité à cette PM et faire rapport des cas de non-conformité ou des incidents de sécurité à leurs chefs de direction générale et d'organisme, leurs directeurs généraux régionaux, leurs directeurs généraux ou leurs directeurs régionaux.

11. Les **utilisateurs** ont la responsabilité de ce qui suit :

    1. assumer les conséquences des gestes qu'ils posent ou omettent de poser en ce qui a trait à la sécurité des TI;

    2. lire, comprendre et respecter la présente PM et le programme de sécurité des

TI du Ministère, qui vise à protéger l'information électronique, les biens de TI et les services connexes dont ils disposent, contre les accès non autorisés, les interruptions, les modifications, les bris et les vols;

3. appliquer à l'environnement de leur poste de travail les mesures de sécurité prévues au programme de sécurité des TI du Ministère;

4. signaler à leur gestionnaire et à leur ASSI, ou au bureau régional de sécurité, toute anomalie et tout manquement, réels ou présumés, en matière de sécurité des TI. L'ASSI ou l'utilisateur doit également communiquer, aussitôt que possible, avec le Bureau de services des TI, au 1-866-995-6030.

7. CONFORMITÉ ET RAPPORTS

Le contrôle relatif à l'efficacité de la présente PM sera assuré selon diverses méthodes, dont, entre autres, des évaluations en vertu du Cadre de responsabilisation de gestion, ainsi que des examens des résultats des vérifications (p. ex. vérifications de sécurité).

Les conséquences d'une non-conformité à la présente PM peuvent comprendre toute mesure prescrite en vertu de la *Loi sur la gestion des finances publiques*.

8. RÉFÉRENCES

Lois et règlements :

- *Charte canadienne des droits et libertés;*
- *Code criminel;*
- *Loi canadienne sur les droits de la personne;*
- *Loi fédérale sur la responsabilité;*
- *Loi sur l'accès à l'information;*
- *Loi sur la Bibliothèque et les Archives du Canada;*
- *Loi sur la gestion des finances publiques;*
- *Loi sur la protection de l'information;*
- *Loi sur la protection des renseignements personnels;*
- *Loi sur la responsabilité civile de l'État et le contentieux administratif;*
- *Loi sur le droit d'auteur;*
- *Loi sur le ministère des Travaux publics et des Services gouvernementaux;*
- *Loi sur les brevets;*
- *Loi sur les licences d'exportation et d'importation;*
- *Loi sur les marques de commerce.*

Publications du Conseil du Trésor :

- Accès à l'information - Politiques et publications;
- Cadre de gestion intégrée du risque;
- Cadre de responsabilisation de gestion;
- Cadre stratégique pour l'information et la technologie;
- *Code de valeurs et d'éthique de la fonction publique;*
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI);
- *Politique d'utilisation des réseaux électroniques;*

- *Politique de télétravail;*
- *Politique sur la gestion de l'information;*
- *Politique sur la gestion des risques;*
- *Politique sur la gestion des technologies de l'information;*
- *Politique sur la sécurité du gouvernement;*
- Protection des renseignements personnels - Politiques et publications.

Publications de TPSGC :

- *Cadre de gestion de TPSGC en matière de communications dans Internet et l'intranet (062);*
- Directive sur la discipline (111 -1)*;*
- Énoncé de TPSGC sur le *Code des valeurs et de l'éthique de la fonction publique;*
- *Gestion des documents et des fonds de renseignements (044);*
- *Gestion du courrier électronique (067);*
- Guide et manuel de gestion du risque;
- Infoguide - Guide ministériel commun de classification et de désignation de l'information et des biens;
- *Politique de gestion intégrée des risques (082);*
- *Politique sur l'attribution et l'utilisation des technologies de l'information (103);*
- *Politique sur la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels (002);*
- *Politique sur la gestion des urgences à Travaux publics et Services gouvernementaux Canada (001);*
- *Programme de la sécurité industrielle (054);*
- *Programme de la sécurité ministérielle (052);*
- *Programme de sécurité du Ministère (051);*
- *Protection des renseignements personnels et particuliers au travail (014);*
- *Signalement des infractions à la sécurité et des manquements à la sécurité réels ou soupçonnés (053).*

Autres publications :

- Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada;
- Effacement et déclassification des supports d'information électroniques;
- Listes de vérification des exigences relatives à la sécurité (LVERS);
- Manuel de contrôle du matériel COMSEC.

9. ANNULATION

La présente PM remplace la version datée du 2010-07-26.

Comme la présente PM a été rédigée en fonction de la structure organisationnelle actuelle de la DGSIT, ainsi que de la *Politique sur la sécurité du gouvernement*, elle pourrait faire l'objet d'une révision si cette structure ou cette politique venait à changer.

10. DEMANDES DE RENSEIGNEMENTS

Directeur, Politique, régie, gestion des connaissances et de l'information
Planification stratégique et architecture de l'entreprise, DGSIT

Portage III 5C2-105
11, rue Laurier
Gatineau (Québec) K1A 0S5

Courriel : TICPolitique.ICTPolicy@tpsgc-pwgsc.gc.ca
Téléphone : 819-934-2733
Télécopieur : 819-956-3669

Le sous-ministre et
sous-receveur général du Canada,

François Guimont

ANNEXE A

DÉFINITIONS

Accès à distance *(remote access)* désigne toute connexion avec les systèmes ministériels de technologies de l'information (TI) qu'il faut établir à partir d'un emplacement à l'extérieur de l'infrastructure actuelle de TPSGC. Les connexions de réseau numérique à intégration de services (RNIS) et celles par modem font aussi partie des connexions à distance.

Accréditation *(accreditation)* est la mesure par laquelle la gestion autorise la mise en exploitation d'un système ou d'un service, après avoir lu les renseignements présentés en vue de la certification et accepté le risque résiduel lié à cette exploitation.

Agent de sécurité de l'unité, ASU *(Unit Security Officer, USO)* est la personne chargée de donner des conseils sur les mesures de sécurité, ainsi que de coordonner tous les volets de la sécurité matérielle, les évaluations de sécurité, les enquêtes de sécurité des utilisateurs, l'émission des cartes d'identité des utilisateurs, ainsi que la réalisation des évaluations de la menace et des risques.

Agent de sécurité des systèmes de l'information*, ASSI* *(Information System Security Officer, ISSO)* est la personne désignée dans le secteur d'activité pour suivre les orientations fonctionnelles et la formation en matière de sécurité des TI que donne la Direction de la sécurité de la TI.

Authentification *(authentication)* est la procédure d'identification d'un ordinateur, d'une source ou d'une personne, puis de vérification de son droit d'accès à des catégories précises d'information; les traitements qui la composent préviennent les transmissions frauduleuses par vérification de la validité d'une transmission, d'un message, d'un ordinateur ou d'une source.

Autorisation et authentification électroniques *(electronic authorization and authentication)* est le procédé électronique permettant : l'identification d'un utilisateur légitime d'un système ou d'un service de TI, puis la vérification de ses droits et permissions (l'autorisation); l'identification des utilisateurs et des dispositifs de systèmes et services de TI, puis la vérification de leur légitimité (l'authentification).

Autorité locale d'enregistrement, ALE *(Local Registration Authorities, LRA)* désigne une personne de confiance, ayant reçu les attestations nécessaires, chargée d'enregistrer les personnes ayant à utiliser l'infrastructure des clés publiques.

Bureau régional de sécurité *(Regional Security Office)* est le bureau chargé de donner des conseils sur les mesures de sécurité, ainsi que de coordonner tous les volets de la sécurité matérielle, les évaluations de sécurité, les enquêtes de sécurité des utilisateurs, l'émission des cartes d'identité des utilisateurs, ainsi que la réalisation des évaluations de la menace et des risques.

Certification *(certification)* est la vérification attestant le respect des exigences relatives à la sécurité d'un système ou d'un service en particulier, ainsi que le bon fonctionnement des contrôles et des mesures de protection.

Code malveillant *(malicious code)* est un programme écrit à de mauvaises fins ou à des fins malveillantes, qui risque d'altérer l'information ou des logiciels, de surcharger les réseaux, d'éliminer des données ou encore de violer la sécurité de systèmes; en font partie les virus, les vers, les chevaux de Troie, les bombes logiques et les bombes à retardement, normalement

activés dans des conditions préétablies ou à un instant prédéterminé. Certains d'entre eux se reproduisent au moyen de réseaux, de disquettes ou d'appareils.

Communication privée *(private communication)* est une communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

Confidentialité *(confidentiality)* réfère à la nature délicate de renseignements ou de biens, exprimée selon une catégorie ou une appellation désignant le degré de préjudice que causerait leur divulgation non autorisée.

Copies de sauvegarde *(backups)* sont des copies de fichiers de données et de logiciels qui permettent, à la suite d'une perte ou d'une corruption, de rétablir les services de TI.

Cryptage *(encryption)* est la transformation de données intelligibles en une suite inintelligible de caractères à l'aide d'un procédé de codage réversible (cf. *cryptographie*).

Cryptographie *(cryptography)* est la discipline traitant des principes, des procédés et des méthodes permettant de rendre des renseignements inintelligibles en vue de les protéger. Elle traite aussi des procédés permettant de restaurer l'intelligibilité des renseignements (cf. *cryptage*).

Cycle de vie du développement de système *(System Development Life Cycle)* désigne les procédures écrites mises en œuvre pour diriger les étapes menant à la mise en production de logiciels et de données (conception, développement, approbation, essai, préparation de la documentation, mise en œuvre, maintenance, protection).

Disponibilité *(availability)* désigne la mesure dans laquelle on peut avoir accès à un système ou à une ressource (par exemple une information) lorsqu'on en a besoin.

Énoncé de la nature délicate *(statement of sensitivity)* désigne une description des exigences relatives à la confidentialité, à l'intégrité ou à la disponibilité qui s'appliquent aux données ou aux biens stockés, traités ou transmis par un système de TI.

Évaluation de la menace et des risques *(Threat and Risk Assessment)* désigne une évaluation de la nature d'actes ou d'événements susceptibles de mettre en danger des renseignements ou biens de nature délicate, de la probabilité qu'ils se produisent et, le cas échéant, de leurs effets.

Incident de sécurité relié aux TI *(IT security incident)* fait référence aux infractions et aux manquements aux règles de sécurité des TI. On parle d'*infractions* s'il y a compromission de données électroniques de nature délicate, ou réduction de la disponibilité ou de l'intégrité de l'information ou si les services de TI ont été affectés; on nomme *manquements* les actes et actes d'omission qui enfreignent une disposition des politiques et des normes de sécurité de TPSGC.

Information essentielle *(critical information)* est l'information dont la divulgation causerait préjudice à une personne ou entraverait une opération ou une activité du Ministère, peu importe qu'elle soit de nature délicate ou non.

Infraction (à la sécurité) *(breach [of security])* est la compromission de biens ou de

renseignements de nature délicate. Sans restreindre la portée de ce qui précède, on considère comme des infractions les divulgations s'étant produites dans des circonstances rendant l'infraction probable.

Infrastructure des clés publiques, ICP *(Public Key Infrastructure, PKI)* désigne le système de délivrance de clés et de certificats cryptographiques, qui permet de sécuriser les transactions électroniques et les échanges de renseignements de nature délicate à l'aide d'un système de tiers de confiance nommés « autorités de certification ». Grâce à l'ICP, on assure la confidentialité, le contrôle d'accès, l'intégrité, l'authentification et la non-répudiation des applications de TI et des transactions commerciales électroniques.

Installations associées aux TI *(IT facilities)* sont les locaux hébergeant du matériel et des services de TI. Les installations forment une partie ou la totalité d'un immeuble : centre de données, salle de serveurs du réseau local, centre de communication, armoire de câblage, espace de travail, etc.

Intégrité *(integrity*) désigne l'exactitude et intégralité de l'information et des biens, et l'authenticité des transactions.

Interopérabilité *(interoperability)* est la capacité des ministères fédéraux de travailler en synergie par l'application de pratiques uniformes de gestion de l'identité et de la sécurité.

Manquement (à la sécurité) *(violation [of security])* désigne tout acte ou acte d'omission qui enfreint une disposition de la *Politique sur la sécurité du gouvernement*. En font partie : le défaut de classifier ou de désigner des renseignements selon cette PM; l'établissement ou le maintien d'une classification ou d'une désignation à l'encontre de cette PM; la modification, la conservation, l'élimination ou le retrait non autorisé de renseignements de nature délicate; l'interruption non autorisée de la circulation des renseignements de nature délicate.

Mode de fonctionnement *(mode of operation)* est une manière de catégoriser les systèmes de TI en ce qui a trait aux contrôles requis, selon la cote et la vérification de sécurité et la connaissance sélective, pour respecter les exigences de la politique sur la sécurité. Le profil d'utilisateur, les caractéristiques du système et les questions de confidentialité permettent de préciser le mode de fonctionnement souhaitable. Il y a trois modes de fonctionnement :

1. Exclusif : Tous les utilisateurs reçoivent la cote de sécurité leur permettant de consulter tous les renseignements sur le système et ont une connaissance sélective de ceux-ci;

2. À niveau dominant de sécurité : Tous les utilisateurs reçoivent la cote de sécurité leur permettant de consulter tous les renseignements sur le système et certains n'ont pas une connaissance sélective de ceux-ci;

3. Multiniveaux : Certains utilisateurs ne reçoivent pas la cote de sécurité leur permettant de consulter tous les renseignements sur le système et certains n'ont pas une connaissance sélective de ceux-ci.

Modems *(modems)* sont des appareils servant à moduler et à démoduler les signaux pour permettre la transmission de données par voie analogique.

Norme de sécurité *(security standard)* désigne un niveau de sécurité jugé suffisant; lignes directrices et exigences relatives à la sécurité dont l'application à l'échelle du gouvernement est approuvée. (Les normes opérationnelles se trouvent dans le Manuel du Conseil du Trésor, tandis

que les normes techniques sont établies par les principaux organismes en matière de sécurité.)

Ordinateurs autonomes *(stand-alone computers)* sont les ordinateurs non connectés à un réseau ou à un autre ordinateur.

Plans de secours *(contingency plans)* sont des énoncés exhaustifs des mesures à prendre avant, pendant et après une catastrophe (situation d'urgence à la source d'une interruption) pour garantir la disponibilité des ordinateurs et des données nécessaires à la poursuite des activités.

Programme de sécurité des TI (*IT Security Program)* est un programme élaboré, mis en oeuvre et maintenu afin de s'assurer que des mesures de sécurité des TI soient adéquatement mises en place à l'égard de toute information organisationnelle qui est recueillie, transformée, transmise, stockée ou diffusée depuis ses systèmes de technologies de l'information.

Propriétaires *(owners)* sont les personnes chargées de prendre les décisions au sujet des fonctions d'un système ou d'un service, et de déterminer quelle information est recueillie et à quelle fin; il s'agit généralement du cadre supérieur responsable de la fonction administrative que remplit le système ou le service.

Renseignements classifiés *(classified information)* sont des renseignements d'intérêt national susceptibles d'être visés par une exclusion ou une exception en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, et dont la divulgation sans autorisation risquerait vraisemblablement de porter préjudice à l'intérêt national. Ces renseignements se répartissent en trois catégories : « confidentiels », « secrets » et « très secrets » (cf. *renseignements désignés*).

Renseignements de nature délicate *(sensitive information)* désignent tout renseignement classifié ou désigné.

Renseignements désignés *(designated information)* désignent touts les renseignements qui, sans être d'intérêt national, sont susceptibles d'être visés par une exclusion ou une exception en vertu de la *Loi sur l'accès à l'information* ou la *Loi sur la protection des renseignements personnels.* Ces renseignements se répartissent dans les catégories suivantes : « Protégé A » (nature délicate), « Protégé B » (nature particulièrement délicate), « Protégé C » (nature extrêmement délicate) (cf. *renseignements classifiés*).

Renseignements détenus *(information holdings)* désignent tout renseignement géré par un ministère, sans égard au support physique de stockage de ces renseignements. En sont exclus les documents dans les bibliothèques fédérales qui n'ont pas été préparés ni produits par ou pour le gouvernement.

Représentant de clients *(client authority)* est un membre d'une direction générale faisant fonction d'interlocuteur unique avec la Direction générale des services d'infotechnologie en ce qui concerne les demandes de changement.

Réseau principal de TPSGC *(PWGSC principal network)* est l'environnement standard pour les activités courantes de TPSGC. C'est là où sont installés la plupart des systèmes d'extrémité et des serveurs de groupe de travail. Cet environnement peut être utilisé pour traiter, stocker et transmettre des renseignements jusqu'au niveau de sécurité « Protégé A ». Dans le cas des renseignements de niveau « Protégé B », leur traitement, leur stockage et leur transmission par le réseau principal sont conditionnels à leur cryptage selon les normes pertinentes approuvées (ICP/MaCLÉ). Enfin, il est interdit de traiter, de stocker ou de transmettre des données de niveau « Protégé C » ou « Classifié » par le réseau principal de TPSGC.

Responsable de la SECOM du Ministère *(departmental COMSEC Authority, DCA)* est responsable de l'élaboration, de la mise en oeuvre, de la tenue à jour, de la coordination et du contrôle d'un programme ministériel de la SECOM conforme à la *Politique sur la sécurité du gouvernement* et à ses normes opérationnelles. La liste des responsabilités précises de ce responsable se trouve dans le Manuel de contrôle du matériel de SECOM (ITSG-10).

Responsables *(custodians)* sont les personnes chargées de l'administration des fonctions, de la structure, des opérations et des données d'un système, d'un service ou d'une installation.

SECOM, sécurité des communications *(COMSEC, Communications Security)* est la protection résultant de l'application de mesures de sécurité (cryptographiques, des transmissions, des émissions, des émanations radioélectriques) au matériel de télécommunication, aux ordinateurs et aux autres appareils de gestion de l'information.

Sécurité des technologies de l'information, STI *(Information Technology Security, ITS)* est la partie de la protection résultant de l'application d'un ensemble intégré de mesures servant à garantir la confidentialité des biens de TI et de l'information stockée, traitée et transmise de façon électronique; l'intégrité de l'information et des processus connexes et la disponibilité des systèmes et services.

Services de TI *(IT services)* est l'accès à un réseau de données et à des services de télécommunications, ainsi qu'aux logiciels utilisés sur le matériel de TI. Par exemple : réseau électronique de TPSGC et services connexes, comme l'accès à des périphériques (p. ex. imprimantes, télécopieurs ou scanneurs); logiciel commercial ou logiciel développé / personnalisé par TPSGC et intégré à un réseau du Ministère ou installé dans un ordinateur; services de gestion des données électroniques et de messagerie (p. ex. messagerie électronique et systèmes de messagerie vocale); Internet; intranet du gouvernement; tout autre service électronique fourni aux utilisateurs de TPSGC par le biais du réseau de TPSGC ou d'un ordinateur d'un dispositif sans fil de TPSGC.

Support d'information amovible *(removal media)* est une carte mémoire, un DVD, un CD-ROM, une disquette, un ruban magnétique, un disque dur ou une clé USB.

Tableau de configuration *(configuration chart)* est un tableau des configurations du matériel, du logiciel et de l'architecture du réseau identifiant tout le matériel, l'ensemble des logiciels et les interconnexions.

Technologies de l'information, TI *(Information Technology, IT)* désignent les disciplines scientifiques, technologiques et d'ingénierie ainsi que les pratiques de gestion servant à la manipulation, à la transmission et au traitement électronique de l'information; les domaines des télécommunications, des réseaux électroniques et du traitement électronique des données, ainsi que leur regroupement en systèmes; leurs techniques et le matériel et les logiciels connexes, de même que leurs interactions avec l'humain et la machine.

Utilisateurs *(users)* comprennent les employés, bénévoles, personnel d'agences de placement temporaire, étudiants, entrepreneurs, consultants et partenaires commerciaux qui ont reçu de TPSGC l'autorisation d'utiliser son réseau, ses systèmes de télécommunication et ses applications, ou encore qui utilisent du matériel et des services de TI dont TPSGC est propriétaire dans des installations du gouvernement fédéral ou à l'extérieur de celles-ci (p. ex. à domicile, en voyage, etc.) pour le traitement, le stockage ou la transmission de données.

ANNEXE B

PRINCIPES DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION DE TPSGC

1. Principes

La sélection et l'application de bons contrôles de sécurité pour un système d'information constituent des tâches importantes, susceptibles d'avoir des répercussions considérables sur les activités et les biens de TPSGC. Par *contrôles de sécurité,* on entend les mesures administratives, opérationnelles et techniques qu'il faut prendre pour protéger la confidentialité, l'intégrité et la disponibilité d'un système et des données qu'il contient. Sauf s'il existe déjà des politiques, directives ou normes propres au Ministère, les principes énoncés ci-dessous doivent guider toutes les pratiques ministérielles :

1. Obligation personnelle de rendre compte

   Tous les utilisateurs, peu importe leur rôle, sont entièrement responsables de leurs actes ou de leur inaction en ce qui concerne la sécurité des technologies de l'information (TI).

2. Sensibilisation

   Les utilisateurs doivent être correctement informés de l'existence et de la portée générale des mesures, des pratiques et des procédures en matière de sécurité de l'information.

3. Classification et désignation de l'information

   Les renseignements doivent être classifiés ou désignés selon le Guide ministériel commun de classification et de désignation de l'information et des biens.

4. Cycle de vie d'un système

   La sécurité des TI doit faire partie intégrante du cycle de vie des applications de tous les systèmes.

5. Proportionnalité

   Les mesures, les coûts, les pratiques et les procédures en matière de sécurité doivent être appropriés et proportionnels à la confidentialité, à l'intégrité et à la disponibilité qu'exigent les biens.

6. Multidisciplinarité

   Les mesures, les pratiques et les procédures pour la sécurité des systèmes d'information portent sur tous les volets de la sécurité des TI : organisation, administration, immeubles, environnement, personnel, matériel, logiciels, communications, opérations.

7. Mise à l'épreuve des environnements

   Considérant que la présomption de sécurité d'un environnement représente un plus grand risque que l'absence de sécurité, aucun environnement n'est jugé sécuritaire tant qu'il n'a pas été certifié par un responsable de la sécurité des TI.

8. Échange de renseignements et interopérabilité

   L’échange de renseignements et l’interopérabilité sont encadrés par des pratiques efficaces et uniformes de gestion de la sécurité et de l’identité.

9. Assurance de protection

   Toutes les mesures, pratiques et procédures de sécurité manuelles ou automatiques doivent être régulièrement employées et mises à l’essai pour garantir leur efficacité.

10. Accès

    Les renseignements et les autres biens ne sont employés que par les utilisateurs le nécessitant, ayant la bonne cote de sécurité ou de fiabilité et détenant l’autorisation pertinente.

11. Séparation des responsabilités

    Dans la mesure du possible, les responsabilités doivent être réparties de manière que nul n’ait l’entière charge d’un processus ou d’une ressource en particulier. Dans certains cas, il faut établir la coresponsabilité d’une ressource pour que sa manipulation ne soit possible que si une autre personne en a été informée.

12. Droit d’accès minimal

    Les utilisateurs de systèmes de TI se voient accorder le minimum de droits d’accès dont ils ont besoin pour exécuter sans entraves leur travail.

13. Éthique

    La sécurité des systèmes de TI doit être appliquée de manière à respecter les droits et les intérêts légitimes de tout un chacun.

14. Intégration

    Pour mettre au point un système de sécurité exhaustif et conséquent, il faut coordonner les mesures, les pratiques et les procédures de sécurité pour chaque système de TI, les intégrer les unes aux autres et les inscrire dans les autres mesures, pratiques et procédures de l’organisation.

15. Manquements et infractions

    Tous les utilisateurs doivent agir rapidement et de façon coordonnée pour prévenir, signaler et réagir aux infractions et aux manquements présumés à la sécurité des TI.

16. Réévaluation

    Considérant que les exigences relatives à la sécurité évoluent, la sécurité des systèmes de TI doit être réévaluée périodiquement.

17. Surveillance

Les pratiques et procédures de surveillance doivent être coordonnées pour garantir la cohérence et l’exhaustivité du système de vérification.

18. Gestion des risques

Il s'agit du processus par lequel les gestionnaires s'informent des vulnérabilités de la sécurité, certifient les mesures de protection et assument le risque résiduel. La gestion des risques doit débuter par une appréciation de la nature délicate des renseignements, qu’on fera suivre d’une évaluation de la menace et des risques, processus itératif comportant des étapes de sélection, de mise en œuvre, de certification, d’accréditation, de mise à jour, de contrôle et de réglage des mesures de protection. La gestion des risques doit prévoir la détermination, l’analyse et l’évaluation des risques, la sélection de mesures de contournement, ainsi que l’établissement et la mise en œuvre de mesures économiques de prévention et de contrôle.

19. Respect de la vie privée électronique

Le droit à la vie privée s’arrête au droit du Ministère de vérifier si les biens électroniques fonctionnent de manière efficace et efficiente, y compris s'ils sont employés à bon escient par les utilisateurs. Le Ministère doit s’efforcer de garantir le respect de la vie privée entre les employés, et entre les employés et d’autres organismes.

20. Gouvernance

Les mesures et les mécanismes de sécurité des TI sont assujettis à la structure de gouvernance de la GI-TI.

21. Mode de fonctionnement

Le mode de fonctionnement des réseaux de TPSGC est selon le mode à niveau dominant de sécurité « Protégé A ». En conséquence, les employés ayant accès au réseau doivent au minimum avoir une cote de fiabilité. Les renseignements de nature plus délicate que ceux classifiés « Protégé A » ne peuvent pas être stockés ni transmis dans les réseaux de TPSGC s’ils ne font pas l’objet de mesures de protection supplémentaires.

ANNEXE C

GESTION DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

1. Délégation des pouvoirs

   Le coordonnateur de la sécurité des technologies de l'information (TI) doit maintenir une relation formelle avec les autres groupes de sécurité du Ministère. Il a la possibilité de déléguer à des employés ou entrepreneurs certaines responsabilités en matière de sécurité; ces responsabilités déléguées doivent être officiellement consignées par écrit.

2. Planification

   Les plans de mise au point de systèmes, de services et d'installations à TPSGC doivent prévoir les activités de mise en œuvre des mesures obligatoires de sécurité des TI.

3. Gestion des risques

   L'application du processus de gestion des risques joue un rôle prépondérant dans la *Politique sur la sécurité du gouvernement* qu'a établie le Conseil du Trésor (CT).

   À moins d'une exemption expresse accordée selon le processus de gouvernance de la GI-TI, la mise en production d'un système, d'une application, d'un serveur, d'un site Web ou d'une installation de TI du Ministère doit être conditionnelle à son accréditation.

   Pour obtenir et conserver ladite accréditation, les propriétaires et les responsables doivent suivre les étapes ci-dessous :

   1. Énoncé de la nature délicate

      Les propriétaires et les responsables doivent préparer et mettre à jour périodiquement des énoncés de la nature délicate, documents présentant les exigences relatives à la confidentialité, à l'intégrité et à la disponibilité des systèmes, des applications, des services et des installations de TI qui traitent, stockent ou transmettent de l'information essentielle ou des renseignements de nature délicate.

   2. Évaluations de la menace et des risques

      Les propriétaires et les responsables doivent préparer et mettre à jour périodiquement des évaluations de la menace et des risques, documents présentant une analyse des vulnérabilités en matière de sécurité et, s'il y a lieu, les mesures de protection nécessaires aux systèmes, aux applications, aux services et aux installations de TI qui traitent, stockent ou transmettent de l'information essentielle ou des renseignements de nature délicate.

   3. Certification

      Les propriétaires et les responsables doivent faire vérifier par le responsable compétent les aspects liés à la sécurité de tous les systèmes, applications, services et installations de TI qui traitent, stockent ou transmettent de l'information essentielle ou des renseignements de nature délicate, de manière à certifier : l'existence et le bon fonctionnement des mesures de sécurité des TI; le respect des exigences relatives à la

sécurité.

4. Examens de la sécurité des TI

À intervalles réguliers, les propriétaires et les responsables doivent réviser leurs énoncés de la nature délicate ainsi que leurs évaluations de la menace et des risques; il en va de même si des modifications à l'environnement de sécurité transforment sensiblement les exigences relatives à la sécurité. Les conclusions de ces examens sont remises au responsable de la certification compétent, qui examinera leur conformité aux politiques et aux normes et prendra les autres mesures jugées nécessaires selon le processus de gouvernance de la GI-TI. Si ce processus débouche sur des modifications substantielles à la configuration, à l'énoncé de la nature délicate, à l'évaluation de la menace et des risques ou aux paramètres de certification (nécessitant peut-être des modifications aux mesures de sécurité), les propriétaires et les responsables ont l'obligation de renouveler l'accréditation.

5. Formation et sensibilisation

Tous les gestionnaires veillent à ce que tous les utilisateurs qui relèvent d'eux soient informés de l'ensemble des politiques, normes et procédures en matière de sécurité des TI qui s'appliquent en fonction de leur rôle et de leurs responsabilités.

Il incombe au coordonnateur de la sécurité des TI d'élaborer un programme ministériel de sensibilisation à la sécurité des TI.

6. Formations et conseils de la Gendarmerie royale du Canada (GRC) et du Centre de la sécurité des télécommunications Canada (CSTC)

Il incombe au coordonnateur de la sécurité des TI de coordonner la tenue de toutes les formations et consultations sur la sécurité des TI que donnent la GRC et le CSTC.

7. Conclusion de contrats de fourniture de services ou de produits de TI

Les gestionnaires doivent veiller à ce que les clauses pertinentes en matière de sécurité des TI soient incluses dans les contrats et protocoles d'entente.

Ils doivent voir en outre à ce que les fournisseurs respectent les exigences contractuelles en matière de sécurité des TI.

À titre d'autorité contractante, TPSGC doit voir à ce que les clauses pertinentes en matière de sécurité des TI soient inscrites dans les contrats qu'il attribue à l'industrie.

8. Vérifications de la sécurité des TI

À intervalles réguliers, les vérificateurs internes mènent des vérifications pouvant aboutir à des recommandations destinées à améliorer les mesures de sécurité des TI.

Le coordonnateur de la sécurité des TI doit recevoir des copies de toutes ces vérifications. Les plans de réduction des vulnérabilités sont assujettis au processus de gouvernance de la GI-TI.

9. Rapports de sécurité des TI aux cadres supérieurs

Le coordonnateur de la sécurité des TI a le devoir d'informer l'agent de sécurité du Ministère

(ASM) de l’état de la sécurité des TI à TPSGC.

10. Protection de l’information

Il est nécessaire d’empêcher les accès non autorisés à l’information en protégeant les supports informatiques et les systèmes, applications, services et installations de TI.

11. Étiquetage de l’information en fonction de la sécurité

Il faut attribuer le niveau adéquat de classification ou de désignation aux renseignements de nature délicate qui sont stockés ou qui sont utilisés par les ressources en TI.

12. Destruction des renseignements classifiés ou désignés

Les propriétaires et les responsables voient à ce que les renseignements électroniques et les biens de TI classifiés ou désignés (y compris ceux mis aux déchets) soient détruits selon les règles prévues au CSTC ITSG-06 – Effacement et déclassification des supports d'information électroniques. Ces règles valent pour les documents imprimés et les renseignements qui se trouvent sur les supports d’information amovibles (p. ex. clé USB, disques durs, disquettes, cassettes, CD-ROM, rubans) et autres supports d’information électroniques.

13. Contrôles d’accès logiques aux systèmes, aux services et aux renseignements

L’accès aux renseignements de nature délicate est strictement restreint au moyen de contrôles d’accès logiques de type physique, informatique et procédural, en plus d’être réservé aux utilisateurs dont les fonctions le nécessitent, qui ont la cote de sécurité pertinente et qui ont obtenu l’autorisation nécessaire.

1. Droits d’accès

   Les propriétaires et les responsables autorisent et établissent les droits d’accès avant que ne soient utilisés les ordinateurs autonomes, les ordinateurs multi-utilisateurs et les réseaux.

2. Identificateurs d’utilisateur

   Les propriétaires et les responsables attribuent un identificateur propre à chaque utilisateur avant de l’autoriser à accéder aux systèmes de TI et aux renseignements. Ces identificateurs ne sont actifs que pour la durée de l’emploi ou de la tâche en particulier.

3. Mots de passe

   Les utilisateurs doivent garder confidentiels leurs mots de passe. La création et la modification des mots de passe sont régies par les normes de sécurité en matière de TI.

4. Gestion des accès

   Les propriétaires et les responsables veillent à ce que les droits d’accès des utilisateurs correspondent à leurs besoins et à leurs autorisations.

14. Message d’accueil

Les propriétaires et les responsables doivent voir à l’affichage du message d’accueil approuvé en matière de sécurité pour que l’utilisateur soit conscient des règles régissant l'accès aux TI. Ce message apparaît une fois par mois à l’ouverture de session, avant que la connexion soit établie.

ANNEXE D

SÉCURITÉ DES APPLICATIONS

1. Mise au point de systèmes et services de technologies de l'information (TI)

   Les gestionnaires de projet veillent à ce qu'un cycle de vie du développement des systèmes, approuvé par TPSGC, et des processus de sécurité des TI s'y rattachant, soient utilisés pour le développement, l'entretien et l'élimination des systèmes et services de TI du Ministère.

2. Installation des logiciels et des applications

   Les utilisateurs doivent faire autoriser par écrit l'installation de tout logiciel (y compris les applications) sur du matériel de TI dont TPSGC est propriétaire. Adressez toute communication à cette fin au Bureau de services des TI, au 1-866-995-6030.

3. Maintenance

   Les propriétaires et les responsables doivent autoriser toutes les activités de maintenance de logiciels.

   Les employés de maintenance sont tenus d'obtenir la cote de sécurité pertinente en fonction de la catégorie de renseignements auxquels chacun peut avoir accès.

   Au cours des périodes de maintenance, il faut établir des mesures de prévention de la copie ou de l'utilisation malveillante des données de nature délicate.

4. Virus et autres codes malveillants

   TPSGC fournit des logiciels antivirus qui protégeront les ordinateurs du Ministère.

   Les utilisateurs doivent suivre les procédures employées par le logiciel antivirus pour détecter les codes malveillants. Les utilisateurs doivent immédiatement communiquer avec le Bureau de services des TI, au 1-866-995-6030, s'ils croient que leur matériel de TI a été infecté par un virus ou un code malveillant.

ANNEXE E

SÉCURITÉ DES OPÉRATIONS DES TECHNOLOGIES DE L'INFORMATION

1. Surveillance opérationnelle

   Les propriétaires et les responsables doivent surveiller l'efficience opérationnelle des ressources de technologies de l'information (TI).

2. Surveillance des menaces et des vulnérabilités

   Les propriétaires et les responsables doivent surveiller les ressources de TI de manière à relever les vulnérabilités et à détecter les cybermenaces; le cas échéant, ils doivent veiller à la prise des mesures d'atténuation pertinentes.

3. Sauvegardes

   Les propriétaires et les responsables veillent à la réalisation et à la mise à l'essai, à intervalles réguliers, de sauvegardes des données électroniques et des logiciels dont ils ont la charge. Les sauvegardes doivent être entreposées à un endroit sécuritaire, à distance des fichiers actifs. Les sauvegardes de renseignements électroniques ou de logiciels essentiels aux opérations, ou encore difficiles à remplacer, doivent être entreposées hors site et conformément à leur niveau de confidentialité.

4. Sécurité des lieux et de l'environnement

   L'accès physique aux supports d'information, aux ordinateurs, aux réseaux locaux et au matériel de télécommunication doit être réservé aux personnes le nécessitant, ayant une cote de sécurité et détenant l'autorisation nécessaire.

   Les salles des ordinateurs, des serveurs du réseau local et des télécommunications doivent faire l'objet de mesures de protection environnementale respectant les normes du gouvernement du Canada.

   1. Construction des installations de TI

      Les gestionnaires de projet font fonction de responsables tout le long de la construction d'une installation de TI; en ce sens, ils doivent veiller à la mise en œuvre de la sécurité des TI.

   2. Zones à accès restreint

      Il est obligatoire d'établir, selon les normes, des zones de sécurité dans le cas des salles où sont traités et stockés des renseignements de nature délicate. On parle notamment des salles hébergeant des ordinateurs centraux, des mini-ordinateurs, des serveurs du réseau local, du matériel de communication, des supports d'information et des salles de télécommunication. L'établissement de telles zones est aussi fonction des évaluations de la menace et des risques.

   3. Protection des biens de TI

Les utilisateurs doivent protéger les biens du gouvernement en leur possession, y compris les renseignements, et ce, où qu'ils soient (lieu de travail, domicile, en déplacement).

4. Emplacement du matériel

Les utilisateurs doivent placer les moniteurs des ordinateurs, les imprimantes et les télécopieurs de manière à empêcher les personnes non autorisées d'y avoir accès, ou encore de consulter les renseignements qu'ils contiennent.

5. Tableau de configuration

Les propriétaires et les responsables tiennent à jour des tableaux de configuration des ordinateurs centraux, des systèmes intermédiaires et des réseaux informatiques ministériels. Ces tableaux doivent être étiquetés en fonction de leur nature délicate.

6. Maintenance

La Direction générale des services d'infotechnologie (DGSIT) a à autoriser toutes les activités de maintenance du matériel de TI et à assurer une supervision adéquate au cours de leur réalisation.

Les employés de maintenance sont tenus d'obtenir la cote de sécurité pertinente en fonction de la catégorie de renseignements auxquels chacun peut avoir accès.

7. Connectivité

La connectivité des télécommunications est autorisée, contrôlée et surveillée par la DGSIT, de manière systématique, selon les politiques et les normes ministérielles en matière de sécurité des TI.

Il est obligatoire de signaler les installations, désactivations et retraits non autorisés du matériel de télécommunication au gestionnaire compétent et au coordonnateur de la sécurité des TI.

8. Utilisation des modems

Il est interdit de brancher des modems sur des ordinateurs en réseau.

Le processus de gouvernance de la GI-TI régit l'approbation de l'installation ou de l'utilisation des modems dans les ordinateurs autonomes, les ordinateurs portatifs et les serveurs de communication dont TPSGC est propriétaire. Dans le cas des systèmes classifiés, il faut employer des connexions par modem approuvées par la sécurité des communications (SECOM).

9. Accès à distance aux réseaux du Ministère

L'accès à distance aux réseaux de TPSGC se fait à l'aide d'une solution approuvée par TPSGC.

10. Transmission de l'information

Les utilisateurs doivent employer des procédures et des produits de cryptage que le

coordonnateur de la sécurité des TI a approuvés. Il est obligatoire de crypter toute transmission de renseignements de niveau « Protégé B », « Protégé C » ou « Classifié », quel que soit le mode de transmission, y compris les suivants :

1. Renseignements électroniques – réseau principal de TPSGC

   Il est autorisé de se servir du réseau principal de TPSGC pour transmettre des renseignements jusqu'au niveau de sécurité « Protégé A ». Dans le cas des renseignements de niveau « Protégé B », leur transmission par le réseau principal est conditionnelle à leur cryptage selon les normes pertinentes approuvées par TPSGC. Enfin, il est interdit de transmettre des données de niveau « Protégé C » ou « Classifié » par le réseau principal de TPSGC.

2. Téléphone

   À TPSGC, le protocole d'interopérabilité des communications sécurisées (dispositifs SCIP) forme le mode autorisé de sécurisation des communications vocales.

   Les utilisateurs doivent se conformer aux Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada (ITSD-01) du Centre de la sécurité des télécommunications Canada (CSTC), ainsi qu'aux directives du Manuel de contrôle du matériel de SECOM sur la détention et l'utilisation des dispositifs SCIP.

3. Télécopieur

   À TPSGC, la transmission sécuritaire par télécopie nécessite l'utilisation d'un dispositif SCIP.

   Les utilisateurs ne doivent pas programmer de numéros non gouvernementaux dans le dispositif de composition rapide du télécopieur, peu importe le degré de confidentialité de l'information transmise.

11. Interconnexion des systèmes informatiques

    Les propriétaires et les responsables procèdent à une évaluation de la menace et des risques afin de déterminer l'incidence de l'interconnexion des systèmes.

12. Internet et intranet

    Les propriétaires et les responsables doivent protéger l'accès à Internet et à l'intranet au moyen d'un dispositif d'accès robuste, comme un pare-feu approuvé.

13. Autorisation et authentification électroniques

    Tous les appareils et les processus servant à l'autorisation et à l'authentification électroniques, ainsi qu'aux signatures numériques, sont assujettis aux règles d'approbation prévues au processus de gouvernance de la GI-TI approprié.

14. Systèmes de messagerie vocale

    Les utilisateurs ne laissent dans la boîte vocale aucun message comportant des renseignements

de nature délicate.

Les propriétaires et les responsables doivent veiller à l'inclusion de contrôles d'accès logiques dans ces systèmes pour empêcher les accès non autorisés.

Ils doivent contrôler régulièrement les systèmes de messagerie vocale pour y détecter des anomalies ou des boîtes vocales inactives.

Les utilisateurs doivent protéger par mot de passe leur boîte vocale.

15. Procédures d'exploitation

Les propriétaires et les responsables voient à l'élaboration et à la mise par écrit de procédures de sécurité relatives à l'utilisation des ordinateurs, puis à leur communication aux utilisateurs.

16. Traitement de l'information

Il est autorisé de se servir du réseau principal de TPSGC pour traiter, stocker et transmettre des renseignements jusqu'au niveau de sécurité « Protégé A ». Dans le cas des renseignements de niveau « Protégé B », leur traitement, leur stockage et leur transmission par le réseau principal sont conditionnels à leur cryptage selon les normes pertinentes approuvées par TPSGC. Enfin, il est interdit de traiter, de stocker ou de transmettre des données de niveau « Protégé C » ou « Classifié » par le réseau principal de TPSGC.

17. Utilisation de *logiciels privilégiés et puissants*

1. Définition

Par *logiciels privilégiés et puissants*, on entend :

1. les logiciels destinés à l'interception, au balayage, à la mise en quarantaine, à l'inspection ou à la manipulation de toute autre façon de données tierces dans un but autre que celui prévu par les parties d'origine;

2. les logiciels servant à contourner les mesures de sécurité mises en place dans l'infrastructure de TPSGC.

Parmi ces logiciels, citons notamment : les systèmes de détection d'intrusion, les balayeurs de ports, les détecteurs de virus, les renifleurs de réseau et les analyseurs de protocole. Cette liste n'est pas exhaustive; en cas de doute, l'utilisateur potentiel est tenu de vérifier la nature de l'outil auprès du coordonnateur de la sécurité des TI.

2. Responsabilité personnelle

L'utilisation de *logiciels privilégiés et puissants* pourrait contrevenir à un certain nombre de lois du Canada, notamment le *Code criminel*, la *Loi sur la protection des renseignements personnels*, la *Loi sur la concurrence* et la *Charte canadienne des droits et libertés*. Le présent énoncé de politique traite des actions susceptibles de déclencher l'application d'une partie ou de l'ensemble de ces lois. Les utilisateurs ayant accès à des *logiciels privilégiés et puissants* sous la garde et la surveillance de TPSGC sont tenus de prendre note que TPSGC ne peut pas autoriser les activités contrevenant à la loi. Les utilisateurs enfreignant le *Code criminel* ou d'autres lois répondront de leurs actions

devant un tribunal.

3. Usages non autorisés

Les actions suivantes sont susceptibles de déclencher une poursuite en justice en vertu du *Code criminel* :

1. l'utilisation non autorisée d'un balayeur de ports contre TPSGC ou d'autres cibles extérieures;

2. l'utilisation non autorisée d'un système de détection d'intrusion;

3. la modification ou la destruction non autorisées de données, (p. ex. le piratage);

4. l'utilisation non autorisée de matériel de TI et de télécommunication spécialement conçu pour intercepter des communications privées;

5. l'altération de données constituant une preuve dans un procès éventuel au criminel, par exemple, la modification des données d'un dossier de piratage;

6. la consultation intentionnelle et non autorisée de données tierces enregistrées sur un support électronique.

4. Autorisation d'utilisation

1. Avant toute utilisation, l'utilisateur d'un *logiciel privilégié et puissant* est tenu d'obtenir une autorisation écrite du coordonnateur de la sécurité des TI. La délivrance de cette autorisation tient compte des besoins opérationnels et de l'existence de procédures de contrôle claires et efficaces garantissant la conformité aux lois et aux politiques. L'autorisation est accordée pour un événement en particulier ou une période donnée et ne s'applique qu'aux personnes dont le nom figure dans le document d'autorisation.

2. Par exemple, sans le type d'approbation mentionné en 4(1), les utilisateurs ne sont pas autorisés à :

- utiliser un logiciel ou un système de TI servant à contourner les mesures de sécurité, ou bien à interférer d'une quelconque façon avec les données ou l'infrastructure de TI du Ministère;

- utiliser un logiciel ou du matériel destiné à intercepter, à balayer, à inspecter, à mettre en quarantaine, à stocker ou à modifier des données tierces faisant partie d'une « communication privée ».

ANNEXE F

GESTION DES INCIDENTS DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

1. Infractions, manquements et incidents relatifs à la sécurité des technologies de l'information (TI)

   L'utilisateur doit signaler à son gestionnaire et à son agent de sécurité des systèmes de l'information (ASSI), ou au bureau régional de sécurité, toute anomalie et tout manquement, réels ou présumés, en matière de sécurité des TI. L'ASSI ou l'utilisateur doit également communiquer, aussitôt que possible, avec le Bureau de services des TI, au 1-866-995-6030.

2. Enquêtes de sécurité des TI

   Le coordonnateur de la sécurité des TI offre du soutien technique aux enquêteurs.