Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Directive sur la gestion de la sécurité ministérielle

Publié : le 07 juil. 2009

© Sa Majesté la Reine du chef du Canada,
représentée par le président du Conseil du Trésor, 2009

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT39-4/2009F-PDF
ISBN : 978-0-660-09629-2

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Directive on Departmental Security Management

Directive sur la gestion de la sécurité ministérielle

1. Date d'entrée en vigueur

1.1 La présente directive entre en vigueur le 1er juillet 2009.

1.2 La période de transition en vue de la pleine mise en œuvre des exigences liées au plan de sécurité ministérielle énoncées aux sections 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.8, 6.1.11, 6.1.12, 6.1.21 et 6.1.23 commencera le 1er juillet 2009 et prendra fin le 31 juin 2012.

2. Application

2.1 La présente directive s'applique:

a. à tous les ministères au sens des annexes I, I.1, II, IV et V de la *Loi sur la gestion des finances publiques* (LGFP) sauf s'ils en sont exclus en vertu d'une loi, d'un règlement ou d'un décret particulier..

3. Contexte

3.1 La gestion de la sécurité est une composante essentielle de la gestion efficace d'un ministère et du gouvernement dans son ensemble. Les activités de sécurité ministérielle doivent être coordonnées centralement et systématiquement intégrées aux opérations courantes afin de s'assurer que les personnes, les informations, les biens et les services soient protégés, que des ministères ne fassent pas courir un risque accru à d'autres ministères ou à l'ensemble du gouvernement et que les activités et les services critiques se poursuivent en cas d'urgence.

3.2 La présente directive définit les rôles et responsabilités des fonctionnaires de ministères qui assistent les administrateurs généraux dans la gestion de la sécurité ministérielle. Ces responsabilités sont à la base d'un processus décisionnel et redditionnel efficace lié aux activités de sécurité ministérielle. Cette directive établit aussi les objectifs minimaux de contrôle de la sécurité qu'un ministère doit atteindre pour s'assurer de remplir son mandat, de mener ses activités et de respecter ses priorités et exigences en matière de sécurité.

3.3 Cette directive doit être lue en parallèle avec le *Cadre principal des politiques du Conseil du Trésor* et la *Politique sur la sécurité du gouvernement* et la *Directive sur la gestion de l'identité*.

3.4 Des exigences obligatoires supplémentaires sont énoncées dans des normes à l'appui des éléments suivants :

- l'assurance de l'information et de l'identité;
- les enquêtes de sécurité;
- la sécurité matérielle;
- la sécurité des TI;
- la gestion des urgences et de la continuité des activités;
- la sécurité des marchés.

4. Définitions

4.1 Pour prendre connaissance de la définition des termes employés dans la présente directive, se reporter à l'annexe A – Définitions.

5. Énoncé de la directive

5.1 Objectifs

La présente directive a pour objectif d'assurer une gestion efficiente, efficace et responsable de la sécurité dans les ministères.

5.2 Résultats escomptés

Les résultats escomptés de cette directive sont les suivants :

- la gestion de la sécurité est une partie définie et intégrante de la gouvernance, des programmes et des services ministériels;
- les ministères adoptent une approche systématique et uniforme dans la planification, la réalisation et la supervision des activités de sécurité;
- des mesures de contrôle minimales sont en place dans les ministères pour appuyer l'interopérabilité et l'échange d'information;
- une gestion active des menaces, des vulnérabilités et des incidents appuie la prestation de services aux Canadiens et les activités du gouvernement;
- les activités de gestion de la sécurité dans un ministère ne font pas courir un risque accru à d'autres ministères ou à

l'ensemble du gouvernement.

6. Exigences

La gestion de la sécurité se fait le plus efficacement avec la participation et la collaboration de l'agent de sécurité ministériel (ASM), des praticiens de la sécurité et des gestionnaires à tous les niveaux. Ceux-ci possèdent les connaissances ministérielles communes qui sont nécessaires pour comprendre les priorités du ministère, l'importance de l'information, des biens, des services et des ressources humaines du ministère ainsi que le niveau de sécurité qui doit être assuré pour les protéger.

6.1 Sécurité ministérielle

Agent de sécurité du ministère (ASM)

L'ASM, qui est désigné par l'administrateur général conformément à la *Politiquesur la sécurité du gouvernement*, doit gérer le programme de sécurité ministérielle et assume la responsabilité de ce qui suit :

Planification

6.1.1 élaborer, mettre en œuvre, surveiller et actualiser un plan de sécurité ministérielle (PSM) qui :

6.1.1.1 renferme une vision commune des exigences de sécurité ministérielle;

6.1.1.2 définit les menaces à la sécurité, les risques et les vulnérabilités afin de fixer un ensemble approprié d'objectifs de contrôle (pour connaître les objectifs minimums de contrôle de la sécurité que les ministères sont tenus d'atteindre, se reporter à l'annexe C – Objectifs en matière de contrôles de sécurité);

6.1.1.3 définit et établit, au besoin, des mesures de contrôle minimales supplémentaires en vue d'atteindre les objectifs en matière de contrôle et d'en arriver à un niveau acceptable de risque résiduel;

6.1.1.4 énonce des stratégies, des objectifs, des priorités et des délais de sécurité pour améliorer la posture de sécurité du ministère;

6.1.2 coordonner, avec les praticiens de la sécurité, la mise en œuvre des mesures de contrôle de sécurité et des autres activités nécessaires à la réalisation des objectifs et des priorités du PSM;

6.1.3 mesurer le degré de réalisation des objectifs énoncés dans le PSM et rendre compte des résultats au comité de gouvernance responsables;

6.1.4 mettre à jour le PSM à la lumière des résultats de la mesure du rendement, de l'évaluation ainsi que des évaluations de risque.

Gouvernance

6.1.5 veiller à ce que les responsabilités, les délégations, les rapports hiérarchiques ainsi que les rôles et responsabilités des employés du ministère à l'égard des responsabilités de sécurité soient définis, documentés et communiqués aux personnes concernées;

6.1.6 établir des mécanismes de gouvernance de la sécurité (p. ex. mettre sur pied des comités, des groupes de travail) pour assurer la coordination et l'intégration des activités de sécurité dans les opérations, les plans, les priorités et les fonctions du ministère afin de faciliter la prise de décisions.

Gestion des risques pour la sécurité

6.1.7 élaborer, documenter, mettre en œuvre et actualiser les processus de gestion systématique des risques pour la sécurité afin d'assurer une adaptation continue aux besoins changeants du ministère et au contexte des menaces;

6.1.8 veiller à ce que les gestionnaires de tous niveaux acceptent officiellement les risques résiduels ou en recommandent l'acceptation. Ces risques sont définis dans le plan de sécurité ministérielle.

Supervision et surveillance

6.1.9 surveiller l'efficacité des mesures de contrôle de sécurité pour faire en sorte qu'elles demeurent à jour et qu'elles satisfont aux exigences de sécurité mentionnées dans les évaluations du risque;

6.1.10 en coopération avec les praticiens de la sécurité, surveiller les changements dans les contextes de menaces et de vulnérabilités afin de s'assurer que les mesures de contrôle de sécurité demeurent pertinentes et que des mesures correctives soient prises au besoin.

Mesure du rendement et évaluation

6.1.11 mesurer le rendement sur une base continue afin de veiller à ce qu'un niveau acceptable de risque résiduel soit atteint et maintenu;

6.1.12 mettre en œuvre un programme d'assurance de la qualité pour s'assurer que les mesures de contrôle de sécurité

satisfont de la manière la plus efficiente et efficace aux exigences de sécurité ministérielle.

Soutien à l'échelle du gouvernement

6.1.13 rendre compte en temps opportun des incidents, des problèmes ou des préoccupations en matière de sécurité aux organismes centraux chargés de la sécurité et aux fournisseurs de services de sécurité (voir l'annexe B – Points de contact pour le règlement des incidents);

6.1.14 coordonner la mise en œuvre des conseils relatifs à l'atténuation fournis par les principaux organismes chargés de la sécurité et faire rapport des mesures présentées au principal organisme chargé de la sécurité concerné;

6.1.15 participer à des tribunes et des comités interministériels, partager les pratiques exemplaires et les leçons tirées et communiquer les besoins du ministère pour obtenir conseils, orientation et services au besoin.

Praticiens de la sécurité

Les praticiens de la sécurité sont les personnes chargées de coordonner, de gérer et de fournir conseils et services à l'égard des activités de sécurité faisant partie d'un programme coordonné de sécurité ministérielle, lesquelles comprennent notamment la sécurité des technologies de l'information (TI), la sécurité matérielle, les enquêtes de sécurité sur le personnel, la planification de la continuité des activités et les opérations régionales de sécurité. Les praticiens de la sécurité sont responsables :

6.1.16 de maintenir un lien hiérarchique fonctionnel ou direct (selon la structure du programme de sécurité du ministère) avec l'ASM afin d'assurer la coordination et l'intégration des activités de sécurité ministérielle;

6.1.17 de sélectionner, de mettre en œuvre et de maintenir des contrôles de sécurité liés à leur champ de responsabilité afin d'assurer la réalisation des objectifs de contrôle;

6.1.18 d'évaluer la mise en œuvre et l'efficacité des contrôles de sécurité, de faire rapport à l'ASM sur la réalisation des objectifs de contrôle et de recommander des mesures correctives pour corriger les lacunes relevées dans la mesure et les évaluations du rendement;

6.1.19 de fournir à l'ASM, aux gestionnaires de tous niveaux et aux employés des conseils d'expert au sujet de l'application et de l'efficacité des contrôles de sécurité liés à leur domaine de compétence;

6.1.20 d'aider l'ASM à concevoir et à dispenser, à l'intention des employés et des gestionnaires de tous niveaux, une formation pour les sensibiliser davantage aux questions de sécurité;

6.1.21 de prendre part aux évaluations des menaces et des risques et contribuer à l'élaboration du PSM au besoin.

Gestionnaires de tous niveaux

Les gestionnaires de tous niveaux sont chargés d'assurer la protection des employés et de préserver les renseignements, les biens et les services dont ils sont responsables. Les gestionnaires sont responsables :

6.1.22 de veiller à ce que les exigences en matière de sécurité soient intégrées à la planification des opérations, aux programmes, aux services et aux autres activités de gestion;

6.1.23 d'évaluer les risques en matière de sécurité, d'accepter officiellement les risques résiduels ou en recommander l'acceptation (ces risques sont définis dans le plan de sécurité ministérielle) et de révaluer périodiquement les risques à la lumière des changements apportés aux programmes, aux activités ou aux services et de prendre des mesures correctives pour corriger les lacunes relevées;

6.1.24 de surveiller la mise en œuvre et l'efficacité des mesures de contrôle de sécurité et de faire rapport à cet égard à l'ASM ou aux praticiens de la sécurité s'il y a lieu;

6.1.25 de s'assurer que les employés appliquent des pratiques de sécurité efficaces dans le cadre des opérations quotidiennes;

6.1.26 lorsque des contrats sont requis, de préciser les exigences en matière de sécurité et les renseignements et les biens classifiés ou protégés dans les documents contractuels et les autres ententes, et de confirmer que les entrepreneurs satisfont aux conditions préalables en matière de sécurité avant de donner accès aux renseignements et aux biens du gouvernement.

Employés

Tous les employés sont responsables :

6.1.27 de protéger les renseignements et les biens dont ils ont la responsabilité, qu'ils travaillent sur place ou non;

6.1.28 d'appliquer des mesures de contrôle de sécurité liées à leur champ de compétence pour veiller à ce que les exigences en matière de sécurité entrent en ligne de compte dans leurs processus, pratiques et programmes courants, ce qui comprend notamment les pratiques administratives et ministérielles comme l'accès à l'information et la protection des renseignements personnels (AIPRP), la gestion des risques, les ressources humaines, les biens immobiliers, la gestion du matériel, les achats, la santé et la sécurité au travail, la gestion de l'information (GI), les TI et les finances;

6.1.29 de signaler les incidents de sécurité en passant par les voies de communication appropriées et de prendre des mesures conformément aux directives de l'ASM et des praticiens de la sécurité;

6.1.30 de continuer à sensibiliser les gens aux questions et aux préoccupations en matière de sécurité afin de s'assurer que leurs actions ne portent pas atteinte à la sécurité du ministère.

6.2 Exigences de surveillance et d'établissement de rapports

Au sein des ministères

- L'ASM est responsable :

  6.2.1 de surveiller la mise en œuvre des activités de sécurité au ministère et de recommander des mesures correctives appropriées à l'administrateur général ou au comité de la haute direction (selon ce qui s'applique) en vue de corriger toute lacune.

- Les gestionnaires de tous les niveaux sont responsables :

  6.2.2 de contrôler la conformité à la présente directive dans leur champ de compétence et de signaler à l'ASM tout incident de sécurité ou infraction à la sécurité.

Par ministère

- L'ASM est responsable :

  6.2.3 de fournir au SCT (sur demande) des éléments probants relatifs à la mise en œuvre et à l'efficacité du programme de sécurité ministérielle (PSM) et du plan de sécurité ministérielle, ce qui comprend les éléments suivants :

  a. description de la gouvernance et de l'organisation du ministère;
  b. éléments de preuve précis touchant la mise en œuvre des mesures de contrôle de sécurité;
  c. résultats de la mesure et de l'évaluation du rendement.

À l'échelle du gouvernement

- Le SCT est chargé :

  6.2.4 de contrôler la conformité à tous les aspects de la présente directive ainsi que l'atteinte des résultats escomptés de diverses façons, notamment au moyen des évaluations effectuées aux termes du *Cadre des responsabilisation de gestion* (CGR) et par l'examen des présentations au Conseil du Trésor, des rapports ministériels sur le rendement et des résultats de vérifications, d'évaluations et d'études.

7. Conséquences

7.1 L'administrateur général est chargé d'enquêter sur les problèmes d'inobservation de la présente directive et d'intervenir à cet égard. Il est aussi responsable de veiller à ce que les mesures correctives appropriées soient prises pour corriger ces problèmes.

7.2 Si le secrétaire du Conseil du Trésor détermine qu'un ministère ne s'est peut-être pas conformé à l'une ou l'autre des exigences de cette directive, il peut demander à l'administrateur général :

7.2.1 de procéder à une vérification ou à un examen – dont le coût sera imputé au niveau de référence du ministère – pour déterminer si les exigences de la présente directive ont été satisfaites; et/ou

7.2.2 de prendre des mesures correctives et de faire rapport sur les résultats qu'elles auront produits.

8. Références

La législation pertinente à cette directive comprend ce qui suit :

- *Charte canadienne des droits et libertés*
- *Code canadien du travail*
- *Code criminel*
- *Loi canadienne sur les droits de la personne*
- *Loi sur l'accès à l'information*
- *Loi sur l'emploi dans la fonction publique*
- *Loi sur la Bibliothèque et les Archives du Canada*
- *Loi sur la gestion des finances publiques*
- *Loi sur la gestion des urgences*
- *Loi sur la protection de l'information*
- *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles*
- *Loi sur la protection des renseignements personnels*
- *Loi sur la statistique*

- *Loi sur le casier judiciaire*
- *Loi sur le service canadien du renseignement de sécurité*
- *Loi sur le système de justice pénale pour les adolescents*
- *Loi sur les immeubles fédéraux et les biens réels fédéraux*
- *Loi sur les relations de travail dans la fonction publique*
- *Règlement canadien sur la santé et sécurité au travail*

Politiques et règlements du Conseil du Trésor pertinents à cette directive :

- *Cadre de gestion intégrée du risque*
- *Cadre de politique sur la gestion des actifs et services acquis*
- *Cadre de politiques en matière de langues officielles*
- *Cadre des politiques de gestion de la rémunération*
- *Cadre principal des politiques du Conseil du Trésor*
- *Cadre stratégique pour l'information et la technologie*
- *Code de valeurs et d'éthique de la fonction publique*
- *Directive sur la gestion de l'identité*
- *Directive sur les marchandises contrôlées*
- *Directive sur les rôles et responsabilités en matière de gestion de l'information*
- *Norme de sécurité et de gestion des marchés*
- *Norme de sécurité opérationnelle – Gestion de la sécurité des technologies de l'information (GSTI)*
- *Norme de sécurité opérationnelle – Programme de planification de la continuité des activités (PCA)*
- *Norme opérationnelle sur la sécurité du matériel*
- *Norme sur la sécurité du personnel*
- *Politique de communication du gouvernement du Canada*
- *Politique en matière d'apprentissage, de formation et de perfectionnement*
- *Politique sur l'accès à l'information*
- *Politique sur l'évaluation*
- *Politique sur la sécurité du gouvernement*
- *Politique sur la gestion du matériel*
- *Politique sur la structure de la gestion, des ressources et des résultats*
- *Politique sur les marchés*
- *Politique sur la gestion de l'information*
- *Politique sur la gestion des biens immobiliers*
- *Politique sur la gestion des projets*
- *Politique sur la gestion des risques*
- *Politique sur la gestion des technologies de l'information*
- *Politique sur la protection contre les incendies, enquêtes et rapports*
- *Politique sur la protection de la vie privée*
- *Politique sur la vérification interne*
- *Politique sur le contrôle interne*
- *Politique sur les langues officielles pour la gestion des ressources humaines*
- *Politique sur les plans d'investissement à long terme*
- *Politique sur les pertes de deniers et infractions et autres actes illégaux commis contre la Couronne*
- *Programme de coordination de l'image de marque*
- *Sécurité et la santé au travail*

Autres instruments de politique pertinents à cette directive :

- Instrument de politique sur la sécurité des communications (COMSEC)

9. Demandes de renseignements

Veuillez adresser toute demande de renseignements au sujet de la présente directive à votre ASM. Pour l'interprétation de la directive, l'ASM devrait communiquer avec la Division de la sécurité et gestion de l'identité.

Annexe A – Définitions

gestionnaires de tous niveaux (*managers at all levels*)
: Cela comprend les superviseurs, les gestionnaires et les cadres supérieurs.

intégrité (*integrity*)
: État de ce qui est précis, complet, authentique et intact.

pour un motif valable (*for cause*)
: Situation où il est déterminé qu'il existe une raison suffisante de révaluer, de révoquer, de suspendre ou de réduire une cote de fiabilité, une autorisation de sécurité ou un accès à des sites.

programme de sécurité (*security program*)
: Ensemble de moyens mis en Œuvre et d'activités liés à la sécurité qui sont gérés dans le but de répondre à des besoins

particuliers et pour obtenir les résultats prévus.

renseignement ou bien protégé (*protected asset or information*)

Un bien ou un renseignement pouvant être visé par une exemption ou une disposition d'exclusion de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* parce que l'on peut raisonnablement s'attendre à ce que sa divulgation compromette l'intérêt non national.

risque résiduel (*residual risk*)

Le risque qui continue d'exister après l'application des contrôles.

Annexe B – Points de contact pour le règlement des incidents

L'ASM ou une autre personne désignée est chargé de signaler les incidents de sécurité et les incidents soupçonnés de constituer une menace nationale ou une menace à une organisation autre que la sienne comme suit :

- Les préoccupations liées à la sécurité nationale, y compris celles en matière de terrorisme, doivent être déclarées au Service canadien du renseignement de sécurité (SCRS), au 613-993-9620.
- Les activités criminelles soupçonnées doivent être déclarées au Centre national des opérations (CNO) de la GRC, un service ouvert 24 heures sur 24, 7 jours sur 7, au 613-993-4460 (les signalements ou les appels peuvent être réacheminés aux organisations locales d'application de la loi s'il y a lieu).
- Les demandes de renseignements concernant les évaluations de l'application de la loi doivent être acheminées par courriel à Soutien opérationnel et services aux clients des Services canadiens d'identification criminelle en temps réel (SCICTR) de la GRC, à l'adresse RTID_ITR@rcmp-grc.gc.ca.
- Les cyberincidents, atteintes à la sécurité matérielle de systèmes ou de services critiques et incidents de sécurité des TI ne faisant pas partie des opérations normales qui causent ou peuvent causer une perturbation ou une réduction de la qualité des services ou de la productivité, ou qui sont caractérisés par une tentative non autorisée, réussie ou non, d'accès dans le but de modifier, de détruire, de supprimer ou de rendre inutilisable tout réseau informatique ou système doivent être signalés selon le Plan de gestion des incidents de TI du GC.
- Les incidents concernant le matériel COMSEC comptable doivent être signalés à l'ASM du ministère où l'incident lié à la COMSEC s'est produit.

Annexe C – Objectifs en matière de contrôles de sécurité

Les ministères sont responsables de sélectionner, de mettre en œuvre, de surveiller et de maintenir des moyens durables de contrôle de la sécurité afin d'atteindre les objectifs en matière de contrôles de sécurité. Les mesures de contrôle de sécurité peuvent être de nature administrative, directoriale, opérationnelle, technique ou procédurale. Les contrôles de sécurité obligatoires et recommandés sont précisés dans les normes et les lignes directrices qui appuient la *Politique sur la sécurité du gouvernement*. Les ministères peuvent prendre d'autres mesures de contrôle de sécurité et se fixer des objectifs de contrôle supplémentaires en se fondant sur les résultats des évaluations des risques.

Assurance de l'information

- L'information est protégée contre les actes non autorisés d'accès, d'utilisation, de divulgation, de modification, de déclassement, de transmission ou de destruction.
- Les renseignements sont définis et classés en fonction du degré de préjudice qui pourrait résulter de la compromission de leur confidentialité, de leur disponibilité ou de leur intégrité.
    - Des renseignements sont définis et classés dans la catégorie « Classifié » (confidentiel, secret ou très secret) lorsque l'on peut raisonnablement s'attendre à ce que leur divulgation non autorisée porte atteinte à l'intérêt national.
    - Des renseignements sont définis et classés dans la catégorie « Protégé » (A, B et C) lorsque leur divulgation non autorisée pourrait raisonnablement porter atteinte à des intérêts autres que l'intérêt national.
    - Des renseignements sont définis et classés dans les catégories « Élevé », « Moyen » et « Faible » lorsque leur divulgation, modification, interruption ou destruction non autorisée pourrait raisonnablement entraîner une atteinte à leur disponibilité ou leur intégrité.
- L'accès à des renseignements classifiés et protégés est limité aux personnes autorisées ayant fait l'objet d'une enquête de sécurité au niveau approprié et ayant expressément besoin d'y avoir accès.
- Seules les personnes autorisées peuvent modifier ou supprimer des renseignements.
- Des mesures de sécurité appropriées sont en place pour l'accès, le stockage, la transmission et le déclassement des renseignements.
- La sécurité de l'information est prise en compte dans toutes les étapes du cycle de vie des renseignements ou du système d'information afin de s'assurer que les exigences liées à la sécurité soient fixées tôt, que les mesures de contrôle de sécurité soient examinées, que la direction donne son autorisation avant le début de l'opération et que l'autorisation soit maintenue par un contrôle continu de la posture de sécurité.

Enquête de sécurité

- Toutes les personnes qui doivent avoir accès à des renseignements, des biens ou des installations du gouvernement se soumettent à une vérification de leur fiabilité et de leur intégrité et, le cas échéant, de leur loyauté ou fiabilité quant à leur loyauté envers le Canada avant d'obtenir leur autorisation d'accès.
- Le processus d'enquête de sécurité est juste et objectif et il respecte les droits de la personne, y compris la vie privée.
- Les personnes sont officiellement informées des privilèges et des interdictions d'accès qui se rattache à leur niveau d'enquête de sécurité avant le début de leurs fonctions, au besoin, au cours du cycle de mise à jour et lorsqu'il y a un changement à leur niveau d'enquête de sécurité, elles signent des formulaires appropriés d'information.
- Les personnes sont traitées de façon juste lorsque leur cote de sécurité est révisée, annulée, refusée, suspendue

temporairement ou abaissée pour un motif valable.
- Les enquêtes de sécurité sont effectuées dans le respect des normes du gouvernement du Canada et peuvent être transférées d'un ministère à l'autre.

Sécurité matérielle

- Les renseignements, les biens et les installations sont protégés contre l'accès, la divulgation, la modification ou la destruction non autorisés, en fonction de leur niveau de sensibilité, de leur pertinence et de leur valeur.
- L'accès aux biens et installations du gouvernement est limité aux personnes autorisées ayant fait l'objet d'une enquête de sécurité au niveau approprié et ayant expressément besoin d'y avoir accès.
- Des relations de gardien à locataire sont définies dans une entente officielle de façon que les responsabilités partagées et individuelles soient attribuées en vue d'atteindre des résultats optimaux au chapitre de la sécurité.
- Les considérations liées à la sécurité sont complètement intégrées au processus de planification, de sélection, de conception, de modification, de construction, d'application, d'exploitation et d'entretien des installations et de l'équipement.
- L'environnement externe et interne d'une installation est conçu et géré de manière à créer des conditions qui, grâce à des mesures de sécurité matérielle, réduisent le risque de violence au lieu de travail, protègent contre l'accès non autorisé, permettent de détecter les tentatives réussies ou non d'accès non autorisé et de mettre en branle une intervention efficace.
- Des contenants, des procédés et des procédures définis ou recommandés dans les normes et directives du gouvernement du Canada sont utilisés pour le transport, la transmission ou la destruction de renseignements et de biens protégés et classifiés.

Sécurité des TI

- Les considérations en matière de sécurité des TI sont pleinement intégrées afin d'atteindre les objectifs opérationnels à chaque étape du cycle de vie du système de TI, y compris à celles de la définition, de la conception, de l'élaboration, de l'exploitation, de l'entretien et du démantèlement.
- Les utilisateurs doivent être identifiés et authentifiés avant d'obtenir accès aux systèmes de TI.
- L'accès aux systèmes de TI et d'information électronique est limité aux utilisateurs autorisés, y compris les types de transaction et de fonction que les utilisateurs autorisés ont le droit d'effectuer, en fonction des exigences opérationnelles et de sécurité.
- La confiance dans la sécurité des systèmes de TI est assurée par ce qui suit :
    - l'évaluation des contrôles de sécurité;
    - la réduction ou l'élimination des lacunes;
    - l'octroi de l'autorisation avant la mise en service;
    - le maintien de l'autorisation.
- La posture de sécurité des TI est constamment maintenue grâce à une surveillance des menaces et des vulnérabilités, à la détection d'activités malveillantes et d'accès non autorisés et à la prise de mesures à la fois préventives et d'intervention pour minimiser les conséquences.
- Des dossiers et des registres de vérification des systèmes de TI sont crés, protégés et conservés pour permettre une surveillance, des analyses et des enquêtes de manière que les utilisateurs puissent être tenus responsables de leurs actes.
- Les données que renferment tous les appareils, les dispositifs et les médias électroniques portables sont protégées puis épurées ou détruites avant la disposition ou la réutilisation de matériel.
- Les communications électroniques sont protégées par des zones de sécurité dans les réseaux et par la défense du périmètre aux limites des réseaux.

Sécurité des marchés

- Les exigences en matière de sécurité sont définies, traitées, formellement documentées, appliquées et surveillées au cours de toutes les étapes de la passation du marché et pendant toute la durée du contrat.
- Les renseignements, les biens, les systèmes et les installations confiés à l'industrie satisfont aux exigences en matière de sécurité de l'industrie et bénéficient d'un niveau adéquat de protection pendant tout leur cycle de vie.

Partage de renseignements et de biens avec d'autres administrations publiques et organisations

- Les renseignements, les biens et les installations confiés à des organisations extérieures au gouvernement du Canada, ou qui sont partagés avec ces dernières, bénéficient d'un degré adéquat de protection pendant tout leur cycle de vie.
- Les renseignements et les biens de tiers confiés au gouvernement du Canada bénéficient d'un niveau de protection adéquat pendant tout leur cycle de vie.
- Des arrangements ou accords documentés énoncent clairement les obligations redditionnelles et les responsabilités respectives des parties, conformément aux normes du gouvernement et de l'industrie, et on les réexamine périodiquement pour vérifier qu'ils sont toujours appropriés et pertinents.

Obtention de services de sécurité auprès d'autres organisations

- Des arrangements ou accords formels sont conclus lorsque des services de sécurité sont obtenus d'une autre organisation.
- Ces accords renferment des dispositions en matière de sécurité qui exposent clairement les obligations redditionnelles et les responsabilités respectives du ministère et du fournisseur de services.
- Une surveillance est effectuée pour vérifier que les arrangements respectent les dispositions en matière de sécurité et sont toujours pertinents ou pour les actualiser au besoin.

Sensibilisation aux questions de sécurité

- Un programme de sensibilisation à la sécurité ministérielle couvrant tous les aspects de la sécurité des ministères et du gouvernement est cré, géré, exécuté et actualisé pour s'assurer de renseigner les personnes et de leur rappeler régulièrement

les questions et les préoccupations liées à la sécurité ainsi que leurs responsabilités à ce titre.
- Les personnes comprennent et assument leurs responsabilités en matière de sécurité et ne compromettent pas la sécurité par inadvertance.

Formation sur la sécurité

- Les ASM, les praticiens de la sécurité ainsi que d'autres personnes ayant des responsabilités particulières au chapitre de la sécurité reçoivent une formation adéquate et actualisée de manière à posséder les connaissances et les compétences nécessaires pour s'acquitter efficacement de leurs responsabilités en matière de sécurité et ne pas compromettre la sécurité par inadvertance.

Gestion des incidents de sécurité

- Des mesures sont prises pour se tenir prêts et intervenir en cas d'incidents de sécurité, pour en atténuer rapidement les incidences et assurer la reprise des activités ainsi que pour prévenir ou minimiser les conséquences et les pertes potentielles.
- Les incidents qui ont ou pourraient avoir des répercussions sur le degré de préparation du gouvernement, sur l'atténuation des incidences, sur les interventions ou sur la reprise des activités à la suite de menaces et de vulnérabilités sont signalés à l'organisme principal concerné chargé de la sécurité ou aux autorités d'application de la loi (voir l'annexe B – Points de contact pour le règlement des incidents) et, au besoin, à d'autres ministères lorsqu'il y a des raisons de croire que l'atteinte à la sécurité provient d'un ministère en particulier.
- Une analyse postérieure à l'incident et un suivi sont effectués, et les résultats sont communiqués à l'organisme principal concerné chargé de la sécurité.

Protection des employés contre la violence en milieu de travail

- Des mesures de protection sont en place pour protéger les employés (et les membres de leur famille si on le juge nécessaire en fonction de l'évaluation des menaces et des risques de certaines situations) contre la violence au lieu de travail à laquelle ils pourraient s'exposer en raison des fonctions qu'ils assument ou dans le cadre de leur travail.
- Les employés exposés à ce risque ont accès à des renseignements et une formation sur la gestion de telles situations.
- Des registres détaillés sont tenus et des déclarations sont prises sur les incidents signalés de violence en milieu de travail.

Inspection de sécurité

- Des inspections de routine sont effectuées aux emplacements/installations ou systèmes dans lesquels sont traités ou entreposés des biens et informations de nature délicate afin d'assurer la conformité aux exigences en matière de sécurité du ministère (p. ex. vérification des aires de bureau pendant les heures à accès limité).
- Des inspections de sécurité sont menées en conformité avec les dispositions des conventions collectives et des lois et des règlements sous-jacents; elles revêtent un caractère raisonnable dans les circonstances, et l'on fait connaître aux employés leurs procédures de déroulement avant de les effectuer.
- Les inspections de sécurité sont menées par des personnes à qui l'on a assigné cette responsabilité et ne ciblent pas de fonctionnaires en particuliers.
- Les violations ou atteintes soupçonnées à la sécurité sont signalées sans délai et font l'objet d'une enquête aux fins de mesures correctives, ou d'une déclaration aux autorités responsables, au besoin.

Enquêtes administratives liées aux incidents de sécurité

- Des enquêtes sont conduites de manière à ne pas compromettre l'évidence, les droits des personnes ou les poursuites civiles ou criminelles.
- Des procédures sont définies et mises en œuvre pour fixer les conditions dans lesquelles se déroulera chaque enquête administrative.
- Les incidents qu'on soupçonne de constituer une infraction criminelle sont signalés aux autorités chargées de l'application de la loi et des protocoles sont établis pour assurer la coopération entre le ministère et les organismes d'application de la loi.
- Les parties à l'enquête sont dûment informées de leurs droits et obligations.

Sécurité dans les situations d'urgence et de menace accrue

- Des plans et des procédures sont en place pour passer à des niveaux de sécurité supérieurs en cas d'urgence et de menace accrue.
- Les ministères peuvent assurer la coordination avec d'autres plans de prévention et d'intervention en cas d'urgence (p. ex. incendie, alertes à la bombe, matériaux dangereux, pannes de courant, évacuations, situations de crise civile) lors d'une situation d'urgence ou de menace accrue.

Planification des urgences et de la continuité des activités

- Des plans d'assurance de la continuité des activités et des plans d'urgence viennent appuyer la récupération et la reprise des fonctions et des services opérationnels essentiels ainsi que des biens et des ressources qui leur sont associés pour assurer la prestation d'un minimum de services sans interruption.
- Les biens et les services critiques du ministère sont définis, analysés et une priorité leur est accordée selon leur caractère essentiel.
- Un répertoire de services critiques et de renseignements connexes, de biens et de dépendances est tenu à jour, et ce répertoire est transmis à Sécurité publique Canada au besoin.
- Des plans de continuité des activités et des stratégies de reprise des activités sont élaborés et des ententes sont conclues pour tous les service critiques.

- Les plans de continuité des activités sont testés et des exercices de préparation sont menés de façon à assurer une intervention et un rétablissement efficients et efficaces.