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

Norme de sécurité relative à l'organisation et l'administration

Publié : le 01 juin 1995

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

N° de catalogue BT39-25/1995F-PDF
ISBN : 978-0-660-17736-6

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: Security Organization and Administration Standard

Norme de sécurité relative à l'organisation et l'administration

1. Introduction

1.1 Objet et portée

Ce document énonce la norme opérationnelle devant servir à l'organisation et à l'administration de la sécurité conformément à la Politique sur la sécurité. La norme comporte des exigences, indiquées par les mots « doit » ou « doivent » dans les phrases apparaissant en italique dans le texte, et des mesures de protection recommandées indiquées par les mots « devrait » ou « devraient ».

1.2 Rôles et responsabilités

Les ministères sont chargés de protéger les renseignements et biens de nature délicate qui relèvent d'eux conformément à la Politique sur la sécurité et à ses normes opérationnelles.

L'autorité contractante est chargée de s'assurer que la Politique sur la sécurité est respectée et que les clauses requises figurent dans les documents contractuels.

1.3 Concept

Il peut être utile pour la direction de la fonction sécurité du Ministère de considérer la sécurité comme un sous-système au sein du système d'administration et de gestion.

- La mise en œuvre du système de sécurité repose sur les éléments suivants :
- Un appui à la politique de la part de l'administrateur général.
- Les services et l'appui des fonctions administratives connexes.
- Des renseignements sur les besoins du Ministère et sur la menace au plan de la sécurité.
- Le bon vouloir de chacun des employés pour assumer les responsabilités en matière de sécurité.

Le système de sécurité comporte des politiques, des procédures et des pratiques favorisant la coordination de la sécurité physique, de la sécurité du personnel et de la sécurité informatique.

L'application du système de sécurité donne lieu aux mesures suivantes :

- L'application de mesures de protection pendant toute la durée de vie utile des biens.
- La formation du personnel au sujet de leurs responsabilités au niveau de la sécurité.
- L'évaluation des mesures de protection pour s'assurer qu'elles demeurent pertinentes.

Ce concept de système de sécurité permet à la fois une certaine souplesse et une approche normalisée. Les éléments particuliers à certains ministères et à certains locaux devraient être notés dans les évaluations de menaces et des risques et se refléter dans les mesures et normes choisies. C'est ainsi qu'un bien pourrait recevoir davantage que la protection minimale requise pour son niveau de classification ou de désignation.

Une autre caractéristique du concept, c'est que si une partie d'un système devient inopérante ou suspecte, on peut lui substituer une autre partie, opter pour une solution de remplacement temporaire, ou augmenter le niveau sécuritaire d'une autre partie du système pour en préserver l'intégrité.

1.4 Conseils

On peut obtenir avis et conseils au sujet des présentes normes en s'adressant aux organisations figurant à l'appendice A.

2. Organisation des documents relatifs à la sécurité

Les présents documents comportent trois volets qui marquent une progression vers des directives et des conseils de plus en plus détaillés. La structure prend la forme d'un triangle, comme dans le tableau 1, où la Politique sur la sécurité se trouve au sommet, les normes opérationnelles au deuxième niveau et la documentation technique au troisième et dernier niveau. La politique et les normes opérationnelles se trouvent dans le volume « Sécurité » du Manuel du Conseil du Trésor. Les organismes-conseils sont chargés d'élaborer la documentation technique ou de troisième niveau.

Tous les documents relatifs à la sécurité suivent le même cheminement en cinq étapes: détermination des besoins, élaboration du mode de réaction, consultation et révision, approbation et promulgation. Le tableau 2 indique où se situe la responsabilité de chaque étape.

Tableau 2 : Documents relatifs à la sécurité - rôles et responsabilités

Processus	Politique sur la sécurité	Normes opérationnelles	Documentation technique
Détermination des besoins	SCT	Organismes-conseils coordonnés par le SCT	Organismes-conseils coordonnés par le SCT
Réaction	SCT	Organismes-conseils coordonnés par le SCT	Organismes-conseils coordonnés par le SCT
Révision et consultation	Comité consultatif	Comité consultatif	Comité consultatif
Approbation	Conseil du Trésor	Conseil du Trésor ou SCT	Organismes-conseils
Promulgation	SCT	SCT	Organismes-conseils

3. Organisation de la fonction sécurité

Chaque ministère est responsable de l'organisation et de la gestion de la fonction sécurité permettant au ministère de mettre en œuvre un programme de sécurité efficace et de respecter les exigences de la politique et ses normes opérationnelles.

L'efficacité de la fonction sécurité dépend du rendement de chaque élément, tel qu'indiqué dans les normes opérationnelles, et de leur coordination. Les ministères devraient donc organiser la fonction sécurité de façon à rendre possibles la planification, la budgétisation, l'orientation, la coordination et l'évaluation dans leur ensemble. Les organisations décentralisées ou les directions ayant des responsabilités distinctes devraient adopter des procédures administratives communes pour la désignation et la classification des renseignements, l'évaluation de la menace et des risques et celle du système de sécurité.

L'efficacité et l'efficience de la sécurité s'appuient sur de saines pratiques administratives générales. C'est particulièrement vrai en ce qui concerne les pratiques d'embauchage et les enquêtes de sécurité, la planification des locaux et du contrôle de l'accès aux installations ainsi que la sécurité au plan de l'administration des systèmes de technologies de l'information et leur sécurité.

Dans un certain nombre de cas, les pratiques administratives suffisent à assurer une protection adéquate des renseignements et des biens de nature peu délicate. Lorsque le danger que des efforts délibérés soient faits pour avoir accès à ce type d'information est faible, mais que les risques d'accidents sont importants, il peut s'avérer inutile de prendre des mesures de protection particulières mais essentiel d'appliquer soigneusement les pratiques administratives. Par exemple, la norme minimale de sécurité en ce qui a trait à l'expédition du courrier de nature peu délicate consiste à utiliser une seule enveloppe et à l'expédier à titre de courrier de première classe, en supposant que l'enveloppe aura été adressée avec soin. On pourrait donner d'autres exemples pour presque tous les aspects administratifs.

Par ailleurs, les pratiques administratives appuient et complètent les mesures de sécurité, quelle que soit la cote de sécurité des renseignements visés. Par exemple, la sécurité des renseignements de nature délicate contenus dans les ordinateurs repose sur la qualité des installations et des pratiques d'exploitation autant que sur les mesures de protection.

Un programme de sécurité efficace dépend également des rapports de coordination établis parmi les gestionnaires de programmes et avec les responsables des autres fonctions administratives, telles la gestion de l'information, les marchés, l'immobilier, le matériel, les finances, l'informatique, les télécommunications, la santé et sécurité, la protection des incendies, l'accès à l'information et la protection des renseignements personnels, la vérification et le personnel.

Pour ces raisons, la politique de sécurité exige que le Ministère nomme un agent de sécurité pour le ministère (ASM) chargé d'élaborer, de mettre en œuvre, d'actualiser, de coordonner et de contrôler un programme ministériel de sécurité en rapport avec la politique et ses normes.

L'ASM devrait, au besoin, avoir directement accès à l'administrateur général afin de signaler les infractions probables aux règles de sécurité ou les actes illégaux, conformément à son mandat.

Pour assurer une communication efficace entre les divers éléments de la sécurité, des liens fonctionnels et hiérarchiques devraient être définis dans la politique ministérielle.

En raison du rôle important que joue le cabinet du ministre dans l'exécution des travaux du ministère, l'ASM veille à maintenir des rapports de travail constants avec les agents chargés de la gestion du cabinet du ministre. Les ASM doivent en outre bien connaître le guide intitulé Pratiques administratives : lignes directrices à l'intention des cabinets des ministres, rédigé par le Secrétariat du Conseil du Trésor.

L'organisation de la fonction sécurité devrait soutenir la coordination des éléments de sécurité ainsi que celle des fonctions administratives connexes.

4. Sécurité de l'information

4.1 Examen des fonds documentaires

Un examen exhaustif des fonds documentaires et autres biens, pour déterminer ce qui doit être classifié ou désigné, devrait être effectué avant d'appliquer toute norme de sécurité.

4.2 Guide de classification et de désignation des renseignements

Les ministères doivent imposer le système de classification et de désignation des renseignements soit au moyen d'un guide

corporatif ou en nommant des agents chargés de cette fonction ou les deux.

Le guide constitue la politique du ministère quant aux renseignements auxquels il souhaite appliquer ses mesures de protection. Le guide énonce :

- Les types de renseignements qui sont jugés de nature délicate.
- Les types de renseignements qui ne sont pas jugés de nature délicate.
- La manière de marquer les renseignements, en indiquant les normes minimales de sécurité qui s'appliquent à chaque groupe.

Le guide devrait aussi indiquer les fonctionnaires qui peuvent classifier ou désigner les renseignements auxquels le guide ne s'applique pas. Les ministères devraient limiter le nombre de fonctionnaires ayant cette autorité et s'assurer que ces responsables ont encore un besoin réel d'exercer cette fonction.

Les renseignements publics ne doivent être ni classifiés, ni désignés.

Pour élaborer un guide de classification et de désignation, les ministères devraient procéder ainsi :

- Examiner systématiquement les fonds documentaires en suivant les critères énoncés dans l'appendice A à la Politique sur la sécurité.
- Assigner la classification sécuritaire appropriée aux renseignements de nature délicate qui sont d'intérêt national.
- Assigner la désignation sécuritaire appropriée aux renseignements de nature délicate autres que ceux d'intérêt national.
- Si possible, préciser la durée de la classification ou de la désignation en indiquant la date ou l'événement à la suite duquel les renseignements seront déclassifiés ou déclassés.
- À intervalles réguliers et en collaboration avec les responsables de l'accès à l'information et aux renseignements personnels, revoir les décisions d'exempter certains renseignements à la suite de demandes découlant de la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels. Ceci vise à s'assurer que les critères de classification ministériels demeurent pertinents et efficaces.

4.3 Liens avec la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels

La plupart des renseignements gouvernementaux sont suffisamment protégés par de saines pratiques de gestion de l'information et du matériel, sans qu'on soit obligé de les classifier ou de les désigner. La Politique sur la sécurité exige que les ministères déterminent le petit nombre de renseignements de nature délicate qui méritent une protection supplémentaire. L'identification de renseignements de nature délicate découle directement des critères d'exemption et d'exclusion de la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels. Ces deux lois établissent le fondement législatif du refus, par les ministères, de communiquer certains renseignements.

Les renseignements qui font exception sont ceux que le Parlement a jugé importants pour la protection soit de l'intérêt national, soit d'autres intérêts envers lesquels le gouvernement a des obligations.

Elles ne s'appliquent pas aux documents confidentiels du Cabinet qui doivent être soit classifiés, soit désignés.

Lorsqu'ils déterminent si des renseignements nécessitent une protection supplémentaire, les ministères ne sont pas tenus de décider définitivement si certains éléments en particulier peuvent faire exception à ces deux lois. Suivant les circonstances ou avec le temps, la situation peut varier. Les ministères doivent plutôt s'assurer que certains types de renseignements pourraient vraisemblablement faire exception. Une telle décision doit reposer sur la détermination du préjudice probable et figurer dans un guide interne de classification et de désignation.

Le système de sécurité actuel s'appuie sur la notion que le gouvernement ne devrait pas consacrer des ressources humaines et financières à la protection accrue de certains renseignements à moins d'avoir de bonnes raisons de croire que ceux-ci font exception ou sont sujets à exemption à la Loi sur l'accès à l'information et à la Loi sur la protection des renseignements personnels. L'objectif est d'abord de déterminer avec précision quels renseignements le ministère a l'obligation de protéger, puis d'établir les mesures de protection minimales appropriées.

Les ministères devraient étudier avec soin les lignes directrices en appendice A à la Politique de sécurité, les dispositions précises de la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels ainsi que les volumes « Accès à l'information » et « Protection des renseignements personnels » du Manuel du Conseil du Trésor afin de déterminer quels types de renseignements devraient être classifiés ou désignés et, par conséquent, nécessiter des mesures de protection. Consultez aussi l'appendice C aux normes décrites afin d'y trouver des conseils supplémentaires sur la classification des renseignements d'intérêt national.

4.4 Types de renseignements désignés

Voici la description de certains types de renseignements désignés.

a) Des renseignements obtenus à titre confidentiel d'autres gouvernements et organismes

Les renseignements non classifiés obtenus à titre confidentiel d'autres gouvernements ou d'organisations internationales d'États, telles que décrites aux sections 13 de la Loi sur l'accès à l'information et 19 de la Loi sur la protection des renseignements personnels, et chapitre 2-8 du volume « Accès à l'information » et chapitre 2-9 du volume « Protection des

renseignements personnels », du Manuel du Conseil du Trésor. Ces renseignements peuvent porter la mention : « PROTÉGÉ - autres gouvernements ». Ils doivent porter la mention indiquant qu'ils ont été reçus à titre confidentiel, en précisant la source, avant de les communiquer à d'autres ministères. Voir les articles 8.5 et 12.9 de ce chapitre pour plus de renseignements à ce sujet.

b) Les renseignements obtenus ou préparés par un organisme d'enquête fédéral

Il s'agit des renseignements policiers obtenus ou préparés par les organismes d'enquête que nomment les règlements de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels. (Alinéas 16.(1)a) de la LAI et 22.(1)a) de la LPRP). De tels renseignements portent sur la détection, la prévention ou la suppression du crime, ou sur l'application des lois fédérales ou provinciales. L'organisme d'enquête fédéral compétent détermine le niveau de protection requis. Les ministères qui reçoivent ces renseignements doivent leur accorder une protection équivalente après avoir consulté l'organisme d'enquête.

c) Les renseignements personnels

Ceux que définit la section 3 de la Loi sur la protection des renseignements personnels sont obligatoirement soustraits à l'application de la Loi sur l'accès à l'information. La Loi sur la protection des renseignements personnels s'applique uniquement à ceux-ci et impose des contrôles juridiques à leur collecte, utilisation, conservation, divulgation et élimination.

On retrouve des renseignements personnels dans l'ensemble des fonds documentaires de la plupart des ministères. On peut repérer ces fonds en utilisant Info Source où conformément à la Loi sur la protection des renseignements personnels, tous les ministères doivent y énumérer les banques et catégories de renseignements personnels qu'ils détiennent.

Les renseignements personnels comprennent ceux qui concernent les fonctionnaires (par exemple, les données sur la paye, les appréciations de rendement et les données médicales). Il faut veiller à ne pas confondre ce type de renseignements avec ceux qui sont décrits au paragraphe 3j) de la Loi sur la protection des renseignements personnels (par exemple, le niveau de classification et l'échelle salariale des fonctionnaires). Cet alinéa impose certaines restrictions concernant la définition des renseignements personnels.

d) Les renseignements commerciaux

Les alinéas 20.(1)a) et b) de la Loi sur l'accès à l'information prévoient des exceptions pour :

- Les secrets industriels de tiers.
- Les renseignements financiers, commerciaux, scientifiques ou techniques de nature confidentielle qu'un tiers fournit à un ministère et qui sont traités comme tels de façon constante par ce tiers.
- Les renseignements qui seraient vraisemblablement susceptibles d'entraîner des pertes ou des profits pour un tiers ou de nuire à sa compétitivité.
- Les renseignements dont la divulgation risquerait vraisemblablement de nuire aux négociations contractuelles ou autres avec un tiers.
- La plupart de ces renseignements proviennent d'entreprises ou d'autres organismes et ce tiers s'attend à ce que les renseignements fournis soient bien protégés, ce que les ministères ont l'obligation de faire. C'est pourquoi ces renseignements devraient être désignés comme autres renseignements de nature délicate, et donc porter la mention PROTÉGÉ.
- Dans certains cas, les tiers inscriront sur les documents les mentions « confidentiel », « renseignements commerciaux confidentiels » ou « fourni à titre confidentiel ». Les ministères devraient les traiter comme s'ils avaient reçu la mention PROTÉGÉ, quelle que soit l'inscription qu'y a apposée le tiers.

e) Les avis

La section 21 de la Loi sur l'accès à l'information prévoit un certain nombre d'exceptions pour certaines catégories de renseignements touchant les processus internes de prise de décisions par le gouvernement quand leur communication pourrait nuire à la réalisation des activités gouvernementales.

On devrait évaluer s'il y a des dommages ou des torts du point de vue de telles exceptions selon l'incidence que la communication de la décision aura sur la capacité du Ministère et du gouvernement d'appliquer des processus similaires de prise de décision, de consulter et de discuter dans le respect de la confidentialité et de donner des avis de bonne foi.

L'information visée par ces exceptions est rigoureusement limitée. Il y a une grande différence entre des avis, des recommandations, des consultations et des délibérations concernant un important programme gouvernemental et l'achat d'équipement de bureau. Le meilleur guide pour exercer la discrétion qui s'impose est le bon sens et le bon jugement.

Il convient aussi de retenir que même si la Loi sur la protection des renseignements personnels ne prévoit aucune exception pour les avis, il est extrêmement important de protéger ceux donnés en vue de décisions touchant des personnes.

4.5 Gravité du préjudice

Lorsque des renseignements sont classifiés dans l'intérêt national, il faut en outre juger du niveau de classification. Ce niveau dépend de la gravité du préjudice qui risque vraisemblablement de survenir par suite d'une atteinte à l'intégrité des renseignements. Voici les niveaux de classification :

- La classification très secret s'applique à un nombre très restreint de renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice exceptionnellement grave à l'intérêt national.

- La classification secret s'applique aux renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice sérieux à l'intérêt national.
- La classification confidentiel s'applique lorsqu'une atteinte à l'intégrité des renseignements risquerait vraisemblablement de porter préjudice à l'intérêt national.

La plupart des renseignements classifiés se retrouveront dans cette dernière catégorie.

Ces niveaux de classification, qui tiennent compte de la définition générale d'intérêt national et de certaines hypothèses pouvant être posées au sujet de menaces générales, exigent l'application de mesures de protection normales et minimales ainsi que l'ajout de mesures de protection supplémentaire fondé sur l'évaluation de menace et risques de tout ministère. On doit aussi appliquer des normes minimales par suite des accords internationaux et des arrangements concernant le partage de renseignements classifiés.

Lorsque les renseignements sont désignés, les niveaux suivants peuvent s'appliquer :

- La désignation de nature extrêmement délicate s'applique à un nombre très restreint de renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice extrêmement grave à des intérêts autres que national, par exemple, la perte de vie.
- La désignation de nature particulièrement délicate s'applique aux renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice sérieux à des intérêts autres que national, par exemple, perte de réputation ou d'avantage compétitif.
- La désignation de nature peu délicate s'applique aux renseignements pour lesquels toute atteinte à l'intégrité des renseignements risquerait vraisemblable-ment de porter préjudice à des intérêts autres que national, par exemple, la divulgation du salaire exact.

Les mesures de protection minimales s'appliquent aussi aux divers niveaux de renseignements désignés. Ces mesures de protection diffèrent de celles s'appliquant aux renseignements classifiés puisqu'elles s'appuient sur des différences au niveau des évaluations de la menace. De plus, en raison de leur caractère spécifique dans chaque ministère, les renseignements désignés de nature extrêmement délicate exigent des mesures de protection spéciales basées sur des évaluations individuelles de la menace et des risques.

4.6 Renseignements personnels de nature particulièrement délicate

Un certain nombre d'exemples de renseignements personnels de nature particulièrement délicate sont présentés plus bas. Cette liste se veut une illustration et une indication et n'est pas exhaustive.

- Les renseignements sur des problèmes médicaux, psychiatriques ou psychologiques.
- Les renseignements recueillis dans le cadre d'une enquête sur une violation présumée de la loi et identifiables comme tels.
- Les renseignements sur l'admissibilité à des prestations d'aide sociale ou sur la détermination du niveau des prestations (ne comprend pas les chèques ou autres effets de paiement).
- Les renseignements fournis sur une déclaration d'impôt.
- Les renseignements décrivant la situation financière d'une personne, à savoir son revenu, ses avoirs, ses dettes, sa valeur nette, ses soldes en banque, ses activités ou antécédents financiers, ou sa solvabilité.
- Les renseignements contenant des évaluations ou recommandations personnelles, des références ou des évaluations du personnel.
- Les renseignements concernant l'origine raciale ou ethnique d'une personne, ses croyances religieuses ou politiques, les associations dont elle fait partie ou son mode de vie.

Il existe une très grande quantité de renseignements personnels de nature délicate partout dans l'administration fédérale; on les retrouve aussi largement concentrés au sein de certains ministères. Étant donné le risque élevé de vol ou de perte de ce type de renseignements, les ministères devraient bien s'assurer de les identifier correctement et d'appliquer à leur endroit des mesures de protection adéquates.

4.7 L'atteinte à la vie privée

Le critère pour déterminer quels renseignements personnels sont de nature particulièrement délicate consiste à évaluer si la divulgation, la suppression ou la modification non autorisées d'un renseignement donné, ou encore sa perte, serait vraisemblablement susceptible de porter atteinte à la vie privée. Ce critère devrait tenir compte des trois éléments suivants :

- Attentes de la personne.

A-t-on précisé certaines conditions à la collecte des renseignements personnels qui porteraient la personne à croire que des mesures spéciales de protection seront prises? Les renseignements sont-ils de nature telle que la personne pourrait s'attendre à ce que le gouvernement prenne des mesures de protection très spéciales sans l'en informer expressément?

- Actualité des renseignements.

Les renseignements sont-ils très actuels et, partant, d'une nature plus délicate ou bien celle-ci a-t-elle diminué avec le temps au point où la divulgation des renseignements, en certaines circonstances, ne causerait aucun préjudice palpable envers la vie privée de la personne?

- Gravité du préjudice.

Si les renseignements sont jugés de nature délicate, peut-on supposer qu'une atteinte à leur intégrité est assortie du risque de causer un sérieux préjudice? On entend par là un tort ou embarras durable qui aura une incidence négative directe sur la carrière, la réputation, la situation financière, la sécurité, la santé ou le bien-être de la personne.

D'autres éléments propres à certaines institutions devraient dans certains cas s'ajouter aux considérations ci-dessus.

4.8 Cueillette de renseignements personnels

Les renseignements personnels recueillis par les ministères au moyen de rapports écrits, de formulaires de demandes, de questionnaires, d'entrevues, etc. requièrent une protection appropriée durant toute leur durée d'utilisation.

Lorsqu'on utilise les renseignements personnels lors d'études ou enquêtes statistiques, le code associant les données aux répondants doit être détruit le plus tôt possible selon un calendrier approuvé par l'Archiviste national.

Les contrats pour la cueillette de renseignements personnels doivent stipuler :

- Qu'on s'engage à protéger les renseignements, à ne les communiquer ultérieurement à aucune autre personne ou organisation et à les utiliser uniquement aux fins précisées dans l'entente.
- Qu'on s'engage à ne communiquer les renseignements qu'aux employés de l'entrepreneur ayant fait l'objet d'une enquête de sécurité en bonne et due forme et qui ont besoin d'y avoir accès.
- Que tout employé auquel on communiquera les renseignements devra signer une déclaration indiquant son engagement, comme condition d'emploi, à respecter la nature délicate des renseignements et à se conformer aux exigences de la Loi sur la protection des renseignements personnels ainsi qu'à toute autre condition imposée par le ministère qui régit l'utilisation des renseignements.
- Que le ministère a le droit de mettre fin au contrat si l'entrepreneur ne respecte pas ses engagements à l'égard de la confidentialité des renseignements.

Voir le chapitre 2-5 pour des renseignements additionnels sur la sécurité des marchés.

5. Sécurité des biens matériels

Selon la politique sur la sécurité, les biens matériels qui sont considérés de nature délicate eu égard à l'intérêt national, doivent être classifiés alors que les biens matériels de valeur ou d'importance qui nécessitent la mise en place de mesure de protection spéciales doivent être désignés. Les biens matériels pouvant nécessiter la mise en place de mesures de protection comprennent : les articles de valeur qui peuvent être subtilisés et revendus, et tout équipement important et de valeur ou tout aspect des immeubles pouvant être la cible de vandales. Ces biens matériels devraient être désignés de « nature délicate ».

Les politiques ministérielles devraient prévoir l'obligation d'établir une liste des biens matériels de nature délicate indiquant l'endroit où ils se trouvent, le type de mesures de protection pouvant s'appliquer et le nom des personnes en ayant la garde. Ces personnes devraient se voir assigner un secteur de responsabilité et faire rapport de tout ce qu'elles considèrent comme une menace à la sécurité des biens dans ce secteur. Les utilisateurs et les personnes qui ont la garde des biens matériels de nature délicate devraient être chargés de les protéger pendant les heures de travail et de suivre les procédures établies pour en assurer la protection à tout autre moment.

Les procédures devraient prévoir le signalement, à l'autorité compétente, de tout dommage causé à des biens matériels de nature délicate ou toute perte confirmée de ces biens. Aucun bien de nature délicate ne devrait être retiré d'un immeuble fédéral ni d'un secteur de responsabilité assigné sans une autorisation en bonne et due forme.

On peut consulter la Direction des systèmes de sécurité de la GRC pour obtenir des conseils sur les mesures à prendre pour assurer la sécurité des biens matériels de nature délicate.

6. Sécurité des technologies de l'information

Les biens de technologies de l'information constituent un type de biens matériels; les éléments des technologies de l'information pouvant nécessiter la mise en place de mesures de protection comprennent :

- L'information, les logiciels, l'équipement et les installations.
- Les services de technologies de l'information.
- Les systèmes de soutien ambiant (par exemple, l'électricité et la climatisation).

Les politiques de sécurité des ministères devraient prévoir des inventaires de technologies de l'information de nature délicate et en attribuer la responsabilité. Les inventaires devraient comprendre les coûts de remplacement des biens de technologies de l'information pouvant servir alors de critère utile au choix de mesures de protection. De plus, on doit préparer, dans le cadre des évaluations de menaces et risques, un énoncé de la nature délicate touchant les biens de technologies de l'information qui indiquent les exigences de la confidentialité, de l'intégrité et de la disponibilité.

Pour de plus amples renseignements, veuillez vous référer au chapitre 2-3 sur la sécurité des technologies de l'information.

7. Protection du personnel

Selon le Code du Travail du Canada, les ministères sont chargés de la santé et de la sécurité de leurs employés en milieu de travail.

(Voir sections 124 et 125, chapitre L-2, Code du Travail du Canada, deuxième partie.) Donc, toutes les évaluations de menace et risques devraient comprendre un volet sur les employés dont le travail peut comporter des menaces à la sécurité. Par exemple, les employés préposés à l'accueil peuvent être confrontés à des membres du public hostiles ou bouleversés, ou les employés dans des postes très en vue peuvent également faire l'objet de menaces de personnes perturbées ou voulant faire les manchettes.

Voir le chapitre 2-2 de ce volume pour des références au sujet de la protection du personnel.

8. Choix des mesures de protection

8.1 Généralités

Les ministères doivent appliquer des mesures de protection en fonction des évaluations de la menace et des risques et d'après les normes de sécurité. Il s'agit ici de s'assurer qu'on tient compte, lorsqu'on applique des normes minimales, des problèmes de sécurité particuliers à la situation.

L'approche de gestion des risques telle que décrite plus bas s'inscrit dans le cadre de la politique gouvernementale de gestion des risques. Pour plus de renseignements, on se référera à la troisième partie du volume « Gestion du matériel, des services et des risques » du Manuel du Conseil du Trésor.

8.2 Renseignements et biens classifiés

Comme il se peut que les renseignements ou biens classifiés soient davantage menacés dans certains lieux ou situations, il faut, outre l'application des normes minimales, prendre des mesures pour s'assurer que la sécurité est adéquate. L'évaluation de la menace et des risques sert à déterminer si des mesures de protection supplémentaires sont nécessaires et, le cas échéant, lesquelles. Ces dernières seront appliquées s'il est rentable de le faire.

Les mentions « CONFIDENTIEL », « SECRET » et « TRÈS SECRET » indiquent la nécessité d'appliquer des mesures de protection de base.

Si les mesures de protection ne s'avèrent pas rentables, on devrait alors envisager d'autres options comme le déplacement des renseignements et biens de nature délicate dans un autre lieu plus sûr.

8.3 Renseignements et biens désignés

Les mesures de sécurité minimales pour le matériel et les technologies de l'information servent à protéger les renseignements et les biens désignés comme n'étant pas de nature délicate ou n'ayant pas une grande valeur. Ces mesures consistent en une protection contre certaines menaces comme l'erreur humaine, le manque d'attention aux procédures indiquées et la malveillance. Il faut faire une évaluation pour s'assurer que les menaces et les risques sont effectivement minimes.

La mention « PROTÉGÉ » indique la nécessité d'appliquer des mesures de protection de base. Les ministères peuvent compléter cette cote « certains y ajoutent la lettre A » pour préciser qu'une protection de base est nécessaire.

Le cas échéant, en vue de contrer d'autres menaces éventuelles, il est recommandé de protéger les renseignements désignés de nature particulièrement délicate par des mesures plus strictes.

Les ministères ont la possibilité d'ajouter la lettre B après la mention « PROTÉGÉ » pour indiquer la nécessité de mesures de sécurité additionnelles. Étant donné la diversité des renseignements désignés de nature particulièrement délicate et des menaces qui les guettent, on ne peut présumer que les mesures de protection seront les mêmes d'un ministère à l'autre.

Par conséquent, on devrait procéder à une évaluation des risques de la sécurité dès lors qu'on communique des renseignements de nature délicate à d'autres ministères. Il appartient aux ministères qui ont recueilli ou produit ces renseignements d'établir les mesures de protection propres à ceux-ci qu'appliquera ensuite le ministère destinataire. Au besoin, on devrait établir une entente écrite avec l'agent de sécurité ministériel du ministère destinataire, et celle-ci devrait lier également tout tiers ayant accès à ces renseignements.

De plus, très peu de ministères détiennent des renseignements désignés dont l'atteinte à l'intégrité pourrait causer un préjudice extrêmement grave, par exemple des pertes de vie ou des pertes financières graves. De tels biens ou renseignements pourraient être menacés par des individus ou organisations très motivés et adroits. Il convient donc d'adopter des mesures de protection additionnelles.

L'ajout de la lettre C après la mention « PROTÉGÉ » signale qu'il faut appliquer des normes strictes particulières. Là non plus, on ne peut présumer que les mesures de protection seront les mêmes d'un ministère à l'autre. Le ministère qui a recueilli ou d'où émanent les renseignements désignés devrait déterminer les mesures de protection nécessaires, et celles-ci doivent faire l'objet d'une entente écrite. Cette entente devrait lier tout tiers ayant accès à ces renseignements.

8.4 Certains exemples de mesures de protection

Certains exemples de mesures de protection minimales pour les renseignements désignés et classifiés sont présentés ci-dessous.

Tableau 3: Quelques exemples de normes minimales de sécurité pour les renseignements PROTÉGÉS

Nature particulièrement

Les activités	Nature peu délicate	Nature particulièrement délicate	Nature extrêmement délicate
Enquête de sécurité relative au personnel	Vérification approfondie de la fiabilité		
Utilisation et entreposage des documents imprimés	Zone de travail, contenant du *Guide du matériel de sécurité* ou l'équivalent, conformément à l'ÉMR.		Zone de sécurité; contenant du *Guide du matériel de sécurité* ou l'équivalent, conformément à l'ÉMR
Transmission de documents imprimés (Canada)	Une seule envelope; courrier de première classe		À certaines conditions; courrier, commis-messager, service de messagerie ou personne autorisée.
Destruction de documents imprimés	Déchiquetage manuel	Déchiqueteuse, répertoriée dans le *Guide du matériel de sécurité*	
Télécopieur	Vérifier que le télécopieur se trouve dans une zone de travail		Vérifier, avec le destinataire présent, que le télécopieur sûr se trouve dans une zone de sécurité
Téléphone	Évaluation par l'usager de la menace et des risques		Télélphone cryptophonique (Type I ou II) dans un lieu approprié
Ordinateur personnel en réseau	Évaluation par le gestionnaire et l'usager de la menace et des risques	Contrôle d'accès physique et logique facultatif ou obligatoire conformément àa l'ÉMIR	Contrôle d'accès physique et logique obligatoire; cryptographie approuvée

Une aide plus détaillée peut être fournie par le biais des normes de travail et techniques. L'évaluation de la menace et des risques doit servir à déterminer le besoin des mesures de protection plus rigoureuses.

Tableau 4: Quelques exemples de normes minimales de sécurité pour les renseignements CLASSIFIÉS

Les activités	Confidentiel	Secret	Très secret
Enquête de sécurité relative au personnel	Cote de sécurité de niveau I	Cote de sécurité de niveau II	Cote de sécurité de niveau III
Utilisation et entreposage des documents imprimés	Zone de travail; contenant du *Guide du Matériel de sécurité* ou l'équivalent, conformément à l'ÉMIR		Zone de sécurité, contenance du *Guide du matériel de sécurité* ou l'équivalent, conformément à l'ÉMR
Transmission de documents imprimés (Canada)	Une seule enveloppe; courrier de première classe		À certaines conditions; courrier, commis-messager, service de messagerie ou personne autorisée
Destruction des documents imprimés	Déchiqueteuse, répertoriée dans le *Guide du matériel de sécurité*		
Télécopieur	Vérifier, avec le destinataire présent, que le télécopieur sûr se trouve dans une zone de travail		Vérifier, avec le destinataire présent, que le télécopieur sûr se trouve dans une zone de sécurité
Téléphone	Téléphone cryptophonique (Type I)		
Ordinateur personnel en réseau	Contrôle d'accès physique et logique obligatoire; cryptographie approuvée		

Une aide plus détaillée peut ëtre fournie dans les normes de travail et les normes techniques.
L'évaluation de la menace et des risques doit servir à déterminer le besoin de mesures de protection plus rigoureuses.

8.5 Renseignements provenant d'autres gouvernements

Les ministères doivent traiter les renseignements de nature délicate provenant d'autres gouvernements ou d'organisations internationales conformément à leurs cotes de sécurité ou aux accords ou ententes entre les deux parties concernées.

L'expression « autres gouvernements » s'entend des gouvernements provinciaux, municipaux ou régionaux et de gouvernements d'autres nations.

9. Gestion des risques de sécurité

9.1 Généralités

La gestion des risques est un processus analytique et logique visant à protéger et, par conséquent, à réduire les risques en ce qui a trait aux biens, aux intérêts et aux employés du gouvernement. Aux termes de la politique de gestion des risques, les ministères doivent identifier, analyser et évaluer les risques, choisir des moyens pour les éviter, élaborer et mettre en œuvre des mesures de prévention et de contrôle rentables. Les ministères doivent également élaborer et mettre en œuvre des plans d'urgence, lorsque cela est approprié. Pour plus de renseignements concernant cette politique, veuillez consulter le volume « Matériel, Services et Gestion des risques » du Manuel du Conseil du Trésor.

Au chapitre de la sécurité, le processus de gestion des risques offre les solutions suivantes :

- Réduire les risques, p. ex. : en améliorant la sécurité.
- Éviter les risques, p. ex. : en modifiant les activités.
- Éliminer ou réduire les mesures de protection non indispensables.
- Contrôler les risques en élaborant des plans de reprise des activités.
- Accepter les risques en connaissance de cause, lorsque cela est approprié.

Aux termes de la politique en matière de sécurité, les ministères doivent effectuer des évaluations de la menace et des risques (ÉMR) relativement aux biens et aux renseignements de nature délicate dans le cadre de la gestion des risques à des fins de sécurité. Le processus d'évaluation de la menace et des risques fait partie intégrante de la gestion des risques en ce qui a trait à la détermination de ce qui doit être protégé, à l'analyse et à l'évaluation de la menace, à l'analyse et à l'évaluation des risques, et à la formulation de recommandations relativement à la gestion des risques. La gestion des risques repose également sur l'examen des décisions de gestion, de leur mise en œuvre et de leur efficacité.

Le système adopté aux fins de la gestion des risques devrait être compatible avec les autres systèmes de gestion des risques appliqués dans le même secteur, p. ex. : pour les incendies.

9.2 Évaluation de la menace et des risques

La conception des équipements et systèmes de sécurité est foncièrement basée sur la nature de la menace. En outre, ceux-ci ont une durée de vie utile qui dépend souvent des progrès technologiques de l'adversaire possible. Une évaluation complète et à jour de la menace visant les renseignements et les biens est donc indispensable pour déterminer si les mesures de protection en vigueur ou proposées sont adéquates.

Lorsqu'on croit qu'une mesure de protection est inadéquate, cela signifie que les renseignements ou biens qu'elle protège peuvent être à risque par rapport aux menaces décelées ou, inversement, surprotégés. Il appartient alors aux responsables de la sécurité d'évaluer les probabilités qu'on profite de ces points faibles (voilà le risque). Ils devraient alors recommander diverses façons de gérer les risques, par exemple accepter les risques, déplacer les renseignements ou biens, faire disparaître la menace, accroître la protection, améliorer les mécanismes de détection et de réaction, et préparer des plans d'urgence.

L'évaluation de la menace et des risques devrait viser le ministère en général ainsi que des installations, des locaux, des systèmes ou des fonctions particulières. Selon la structure du ministère, il faudrait que, dans le cadre d'une évaluation générale, on réunisse et analyse les évaluations particulières. De plus, l'évaluation générale devrait porter sur les menaces qui pourraient avoir des répercussions sur l'ensemble du ministère ou sur les dangers qui constituent une menace aux installations, locaux, systèmes ou fonctions. On élaborera ainsi une évaluation complète et détaillée qui pourra servir à renseigner rapidement l'administrateur général, au besoin.

On devrait également mettre sans tarder à la disposition des responsables des évaluations particulières les renseignements concernant une menace générale. Par exemple, on entend par menace générale tout événement qui pourrait survenir par suite de changements prévus à une loi visant les programmes d'un ministère.

Les évaluations particulières devraient être suffisamment détaillées pour servir de fondement aux recommandations destinées au gestionnaire responsable. Les mesures de sécurité et les procédures d'urgence doivent être prises en compte lors de ces évaluations.

Les évaluations de la menace et des risques devraient être examinées régulièrement et révisées lors de circonstances qui pourraient résulter en une menace accrue, par exemple lors de l'introduction de nouvelles politiques, de réinstallations, de réorganisations ou de changement de technologies.

Le processus ci-dessous n'a pas pour objet de limiter les opérations de sécurité propres à un ministère ou de restreindre son accès à l'information sur les sources de menaces et de risques.

Voir l'article 2.3 du chapitre 2-3 pour des renseignements supplémentaires touchant le processus d'évaluation de la menace et des risques relatif aux technologies de l'information.

9.3 Processus

L'évaluation de la menace et des risques comporte les quatre étapes suivantes :

- Préparation : déterminer ce qu'il faut protéger et définir la portée de l'évaluation.
- Évaluation de la menace : déterminer contre quoi il faut assurer la protection.
- Évaluation des risques : déterminer si les mesures actuelles ou projetées sont appropriées.
- Recommandations : déterminer ce qu'il faudrait faire pour avoir la protection appropriée.

Vous trouverez ci-dessous un aperçu de chacune de ces quatre étapes.

Préparation

La première étape de l'évaluation consiste à repérer les renseignements ou les biens à protéger éventuellement et de déterminer la portée de l'évaluation.

L'énoncé de la nature des activités de l'organisation aidera à déterminer l'importance et la valeur des données et des biens et

de juger si ces derniers sont de nature délicate.

Évaluation de la menace

La menace qui concerne spécifiquement les renseignements et les biens classifiés devrait être évaluée afin de déterminer si elle est faible. Si c'est le cas, on passe à l'étape suivante qui consiste à évaluer l'application des mesures de protection minimales prescrites par les normes. Des conditions spéciales pourraient justifier l'adoption de mesures de protection accrues ou

différentes, par exemple, lorsque des renseignements ou biens classifiés sont expressément visés ou sont situés dans un environnement hostile.

La menace qui concerne spécifiquement des renseignements ou des biens désignés, le personnel ou encore les systèmes ou services d'information désignés devrait faire l'objet d'une description détaillée. On recommande de se poser les questions usuelles : « qui, quoi, où, quand, comment, pourquoi ». On devrait aussi consulter les documents de sécurité du ministère portant sur les infractions et les manquements à la sécurité. On devrait enfin se renseigner sur les difficultés rencontrées avec d'autres installations similaires ou avoisinantes et d'autres systèmes.

On devrait être particulièrement vigilant concernant certains moments ou certaines manipulations où les renseignements et biens sont les plus vulnérables (par exemple les intervalles entre les heures d'accès libre et celles d'accès contrôlé, ou lors des transits).

Si possible, les évaluations particulières devraient donner des précisions sur les menaces visant le ministère dans son ensemble et être examinées par un responsable de la sécurité pour le ministère ou la région.

On peut obtenir des conseils sur la nature des menaces de plusieurs sources :

- Dans les cas d'évaluation d'espionnage, de sabotage ou de menace de terrorisme dont la cible serait les renseignements et biens du ministère, tels que spécifiés à la section 2 de la loi sur la SCRS, communiquez avec la SCRS.
- Quant aux renseignements sur les menaces et les conseils sur les évaluations de menace et risques portant sur des sujets criminels, la sécurité matérielle, la sécurité des ordinateurs et autres aspects pertinents de la sécurité des technologies de l'information, communiquez avec la GRC.
- Quant aux renseignements sur les menaces à l'endroit de la COMSEC ou tout autre aspect pertinent de la sécurité des technologies de l'information, communiquez avec le CST.

Voir l'appendice A pour les adresses de ces organismes.

Les ministères qui ont à l'étranger des installations renfermant des renseignements et biens de nature délicate devraient maintenir des contacts avec le ministère des Affaires étrangères et du Commerce international, par l'entremise de leur bureau de sécurité. Il faudrait consulter les gestionnaires responsables de la santé, de la sécurité et des mesures d'urgence au sujet de menaces comme l'incendie qui posent aussi un problème de sécurité.

Après avoir défini les menaces suffisamment en détail, il est nécessaire ensuite d'évaluer la probabilité et les conséquences qui en découleraient.

Probabilité

On devrait évaluer la probabilité de réalisation d'une menace selon qu'elle est « faible », « moyenne » ou « élevée ». « Faible » signifie qu'il n'y a aucun précédent et qu'il est peu probable que la menace se concrétise. « Moyenne » signifie qu'il y a des précédents et que la menace est vraisemblable. « Élevée » signifie qu'il y a d'importants précédents et que la menace est fort probable. On peut employer le terme « sans objet » pour indiquer que la menace n'est pas pertinente dans une situation donnée.

Diverses méthodes permettent d'assigner des valeurs numériques aux niveaux estimés de menace; elles sont souvent compliquées par contre et doivent faire l'objet d'une interprétation pour être utiles. Il est donc recommandé d'employer des termes descriptifs.

Conséquences

Lorsqu'on a établi le degré de probabilité de réalisation d'une menace, il peut être utile d'en déterminer les conséquences éventuelles. En fait, cet exercice consiste à relever à nouveau les renseignements et les biens devant être protégés, en mettant l'accent sur les conséquences lorsque l'intégrité est compromise.

Dans le cas des renseignements et biens classifiés, on parlera de conséquences « graves », « très graves » et « exceptionnellement graves », en référence aux trois niveaux de classification.

En ce qui concerne les renseignements et les biens désignés, le personnel ainsi que les services désignés les conséquences devraient être classées comme suit : « perte de confiance », « atteinte au caractère confidentiel », « perte de bien » ou « perte de service ».

Évaluation des risques

La prochaine étape consiste à évaluer les aspects vulnérables face à une menace et qui feraient que cette dernière peut être dommageable. Évaluer les mesures de protection actuelles et proposées comme entièrement satisfaisantes; satisfaisantes dans l'ensemble, ou insatisfaisantes.

Il est recommandé aux ministères d'élaborer une liste de contrôle sur les mesures de sécurité. Il faudrait noter tout aspect du système de sécurité qui n'a pas été évalué.

Les ministères peuvent obtenir l'aide des organismes-conseils pour l'évaluation des mesures de protection. Idéalement, on aura déjà procéder à une évaluation de la menace avant de solliciter de l'aide à cette étape. Si la chose n'est pas possible, on devrait demander de l'aide pendant tout le processus d'évaluation.

Recommandations

L'évaluation de la menace et des risques devrait être suivie d'un rapport à la gestion. Le rapport devrait stipuler des recommandations, présentées par ordre de priorité, en vue de réduire ou d'éliminer les risques à la sécurité, et indiquer aussi une description des ressources nécessaires, notamment en ce qui a trait aux finances, au personnel, au matériel et au temps.

Une évaluation utile de la menace et des risques donne au gestionnaire une idée juste des mesures de protection du local ou du système concerné et l'aide à prendre une décision informée au sujet des mesures de protection à appliquer ou retirer.

La page suivante présente, à titre d'exemple, un sommaire d'une évaluation de la menace et des risques.

10. Accès sélectif

L'un des principes fondamentaux de la Politique sur la sécurité est de limiter l'accès aux renseignements de nature délicate aux personnes dont les fonctions l'exigent, c'est-à-dire à celles qui doivent prendre connaissance des renseignements. Alors que les enquêtes de sécurité résultent en l'accès à des renseignements de nature délicate dont le niveau de confidentialité peut varier, l'application du principe de l'accès sélectif limite l'accès dans ces niveaux à certains articles, sujets ou types de renseignements ou de biens de nature délicate. Les employés n'ont pas le droit d'accéder aux renseignements uniquement parce que cela leur conviendrait ou en raison de leur statut, de leur rang, de leur poste ou de leur niveau d'autorisation.

Le principe de l'accès sélectif peut être mis en œuvre de différentes façons, y compris par l'isolement matériel et le contrôle de l'accès aux renseignements, la production de listes de personnes qui peuvent consulter certains types de renseignements, le marquage des renseignements afin de préciser qui peut y avoir ou non accès, et l'établissement de méthodes de contrôle obligatoires ou facultatives sur les systèmes de technologie de l'information.

Parmi les autres moyens de contrôler l'accès aux renseignements, on compte la compartimentation de renseignements de nature délicate associée à des exposés détaillés en matière de sécurité, les compte rendus, ainsi que l'engagement écrit d'assurer des responsabilités connexes en ce qui a trait à la sécurité.

Il appartient au ministère qui produit des renseignements ou qui acquiert des biens de nature délicate de les assujettir au principe de l'accès sélectif.

11. Marquage des renseignements

Les renseignements classifiés doivent être marqués ou identifiés d'une quelconque façon au moment de leur création ou de leur cueillette, afin de signaler aux personnes qui s'en serviront la nécessité de leur accorder un degré de protection donné.

Les renseignements désignés devraient être marqués au moment où ils sont créés ou recueillis. En outre, des renseignements désignés doivent être marqués quand l'unité organisationnelle qui les a créés ou recueillis doit les communiquer à d'autres. Font uniquement exception à cette règle générale les renseignements de nature courante qui concernent la personne et l'organisme auxquels on les communique. Par exemple, il est inutile de marquer un chèque qu'on envoie à une personne ou à son représentant officiel.

L'appendice D présente les normes concernant le marquage des renseignements classifiés et désignés.

12. Déclassification et déclassement

12.1 Généralités

Les renseignements doivent être classifiés ou désignés seulement pour la période pendant laquelle ils doivent être protégés; par la suite, ils seront déclassifiés ou déclassés.

Cette exigence reconnaît le fait que les renseignements classifiés ou désignés cessent d'être de nature délicate avec le temps ou à la suite d'un événement précis. Lorsque la communication des renseignements n'apparaît pas susceptible de porter préjudice aux intérêts en cause, comme l'indiquent les dispositions pertinentes de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, il faut les déclassifier. Ce processus contribue à assurer l'intégrité globale du système de sécurité et permet de communiquer rapidement et sans formalité les renseignements que demande le public.

Le guide de classification et de désignation du ministère devrait conférer le pouvoir de déclassifier ou de déclasser des

renseignements.

12.2 Déclassification et déclassement automatiques

Lorsque c'est possible, les ministères devraient prévoir une date ou un événement précis pour leur déclassification ou déclassement automatique au moment où l'information est créée ou recueillie.

Une date d'expiration automatique de dix ans devrait s'appliquer aux renseignements secrets, confidentiels et désignés de nature peu délicate, en plus des dates et des événements particuliers qui entraînent la déclassification. Toutefois, cette date ne s'appliquerait pas aux renseignements classifiés très secret ni aux renseignements désignés de nature particulièrement délicate (par exemple les dossiers médicaux) ou extrêmement délicate (par exemple les renseignements protégeant les témoins).

Les risques découlant de l'utilisation d'une date d'expiration automatique sont acceptables compte tenu du fait que retirer une classification d'un document n'est pas synonyme de rendre le document public. Le processus normal d'examen de toute demande d'accès demeurerait en vigueur.

12.3 Renseignements partagés

L'obligation de déclassifier ou de déclasser des renseignements de nature délicate s'applique également aux renseignements fournis entre ministères. Dans la mesure du possible, avant de déclassifier ou de déclasser des renseignements provenant d'un autre ministère, ce dernier doit être consulté. Le ministère d'où proviennent les renseignements peut être représenté par le bureau d'origine.

On peut transférer des renseignements au ministère ou au gouvernement qui les a produit pour qu'ils y soient déclassifiés ou déclassés. La plupart du temps, toutefois, il est plus pratique, surtout lorsque les renseignements sont très nombreux, de simplement consulter le gouvernement ou le ministère concerné pour savoir s'il convient de les déclassifier ou de les déclasser.

Dans les cas où il est impossible de consulter le ministère d'origine, les ministères devraient élaborer une procédure de rechange et l'intégrer à leurs guides de classification et de désignation. Il sera nécessaire de le faire, notamment lorsque le ministère qui aura produit les renseignements visés aura été démantelé ou réorganisé de telle façon qu'il soit rendu impossible de le consulter avec efficacité ou efficience.

La décision de déclassifier un document provenant d'un autre ministère ne devra pas être prise de façon inconsidérée. Dans les cas où la consultation avec le gouvernement ou le ministère d'origine ne sera ni pratique ni possible et où il subsistera un doute quant à la nécessité de maintenir des mesures de protection, la procédure devra exiger que l'on consulte les agents compétents. Par exemple, le coordonnateur de l'accès à l'information sera en mesure d'indiquer si les exemptions ou les exclusions continuent d'être applicables.

12.4 Demandes de communication

À la suite d'une demande présentée en vertu des lois pour obtenir des documents qui ont été classifiés ou désignés, le coordonnateur ministériel responsable de l'accès à l'information et la protection des renseignements personnels devrait faire un examen attentif des renseignements avec les responsables visés afin de déterminer s'il y a lieu de demander une exception et s'il y a lieu de tenir une consultation interministérielle.

Toute décision de refuser la communication totale ou partielle d'un document doit reposer uniquement sur les dispositions pertinentes des deux lois en vigueur au moment où la demande est présentée et non pas sur la classification ou désignation sécuritaire, même accordée récemment.

Il est possible de scinder des documents qui ont été demandés en vertu de l'une ou l'autre des deux lois. On peut ainsi décider de prélever les renseignements classifiés ou désignés d'un document examiné à la suite de la présentation d'une demande de communication formelle. Le cas échéant, le document original, dont on a communiqué une copie partielle, demeure classifié ou désigné. Lorsqu'un document complet peut être communiqué, on doit d'abord le déclassifier et le marquer en conséquence.

Les renseignements personnels divulgués en vertu de la Loi sur la protection des renseignements personnels doivent aussi être examinés car certains peuvent conserver une désignation comme renseignements de nature délicate.

Tenant compte des décisions découlant des demandes faites en vertu des deux lois, on devrait revoir à intervalles réguliers le guide ministériel de classification des renseignements.

12.5 Transfert de fonctions

Lorsqu'on transfère des fonctions d'un ministère à un autre en même temps que des renseignements de nature délicate, le destinataire est réputé être le ministère d'origine des renseignements.

12.6 Renseignements transférés aux Archives nationales du Canada

Il est prévu que les ministères transféreront aux Archives nationales du Canada les renseignements de nature délicate pour lesquels la période de conservation a expiré et qui, d'après l'Archiviste national, ont encore une valeur historique ou archivistique.

Les ministères doivent élaborer des accords avec les Archives nationales du Canada afin de déclassifier ou déclasser les renseignements de nature délicate confiés aux Archives. Ces accords doivent tenir compte des conseils prodigués par les ministères d'origine qui préciseront quand il devra y avoir consultation entre eux et les Archives.

Ce qui précède ne s'applique pas aux documents inactifs conservés dans les centres de documents des Archives nationales. Les ministères qui les y entrepose garde le contrôle des documents.

12.7 Institutions abolies

Lorsqu'un ministère cesse d'exister sans que ses fonctions soient transférées à un autre, ses documents doivent être transférés aux Archives nationales du Canada qui assurera leur déclassification ou leur déclassement.

Pour les renseignements qui proviennent d'un ministère aboli, chaque ministère qui en détient des copies est réputé être le ministère d'origine aux fins des normes. Ce ministère peut alors les déclassifier ou les déclasser après avoir consulté les autres ministères intéressés.

12.8 Examen

Les ministères devraient suggérer aux utilisateurs ou aux sources de renseignements de nature délicate qu'ils en vérifient la nature de façon régulière. Au besoin, les renseignements seront déclassifiés ou déclassés et marqués en conséquence.

12.9 Renseignements obtenus d'autres gouvernements

Les renseignements classifiés obtenus de gouvernements étrangers, provinciaux, municipaux ou régionaux, ou d'organismes internationaux doivent être déclassifiés ou déclassés en conformité avec les accords ou ententes convenus avec ces gouvernements ou organismes. Par exemple, la convention régissant les renseignements classifiés du gouvernement britannique fournis au gouvernement du Canada stipule que leur déclassification ne peut être envisagée que 30 ans après leur création.

Les consultations entre ministères et gouvernements étrangers ou organismes internationaux à propos de la déclassification ou du déclassement de renseignements devraient normalement être coordonnées par la Direction générale des services de sécurité au ministère des Affaires étrangères et du Commerce extérieur. La consultation ne devrait se faire directement que lorsqu'un système de liaison acceptable a été établi. Le ministère des Affaires étrangères et du Commerce extérieur devrait être tenu au courant des consultations.

12.10 Renseignements cryptographiques classifiés

Le Centre de la sécurité des télécommunications du ministère de la Défense nationale a la responsabilité d'établir, en consultation avec les ministères concernés, des procédures pour l'examen systématique des renseignements cryptographiques classifiés en vue de leur déclassification ou déclassement. Les ministères doivent consulter le CST avant le déclassement ou l'émission de renseignements ou de documents COMSEC publics produits, diffusés ou publiés par le CST. Cela comprend les renseignements et les documents antérieurs à 1975, époque où le CST était la Direction des communications du Conseil national de recherches (DCCNR).

12.11 Renseignements classifiés du renseignement de sécurité

Le Service canadien du renseignement de sécurité a la responsabilité d'établir, en consultation avec les ministères concernés, des lignes directrices, règles et pratiques spéciales pour l'examen systématique, en vue de sa déclassification ou de son déclassement, des renseignements classifiés qui portent sur les activités du renseignement définies dans la Loi sur le Service canadien du renseignement de sécurité, ainsi que l'information traitant des sources ou méthodes de renseignement. Au besoin, le Centre de la sécurité des télécommunications, le ministère de la Défense nationale, le Bureau du Conseil privé et le ministère des Affaires étrangères et du Commerce extérieur sont chargés d'établir les lignes directrices, règles et pratiques concernant les renseignements classifiés qu'ils ont produits ou qui relèvent d'eux.

12.12 Documents confidentiels du Conseil privé de la Reine

Les documents confidentiels du Conseil privé de la Reine qui sont classifiés et les documents administrés dans le cadre du système des dossiers du Cabinet doivent rester classifiés pour une durée de 20 ans. Il est très rare que ces documents soient déclassifiés ou déclassés plus tôt; après 20 ans, ils peuvent l'être, conformément aux normes énoncées dans cette section.

12.13 Révision des mentions

Le changement d'une mention de sécurité devrait être fait à l'encre, daté et paraphé par la personne responsable. Lorsque le changement s'appuie sur une autorisation écrite, il faudrait le noter sur le document. Cela vaut particulièrement pour les documents qui proviennent d'autres gouvernements ou ministères ou d'organismes internationaux.

Pour les renseignements qui ne sont pas conservés sous la forme d'un texte (par exemple les données informatisées), la correction des mentions de sécurité devrait être adaptée en conséquence. Habituellement, on marque le contenant dans lequel se trouvent les renseignements. Lorsque c'est techniquement possible, les institutions devraient toutefois marquer les renseignements mêmes de façon indélébile.

13. Partage des renseignements de nature délicate avec d'autres gouvernements et organisations

Les ministères doivent élaborer des accords écrits afin d'assurer la protection appropriée aux renseignements de nature délicate partagés avec d'autres gouvernements et organisations. (L'expression « autres gouvernements et organisations » se réfère à ceux qui ne sont pas assujettis à la Politique sur la sécurité mais avec lesquels on partage des renseignements de nature délicate).

Dans la plupart des cas, on prévoit qu'il y aura généralement une entente cadre entre le gouvernement fédéral et l'autre gouvernement ou organisation intéressé. Par cet accord, on devrait s'engager à protéger convenablement les renseignements, à en limiter l'utilisation, à en contrôler la communication à des tiers et à informer les usagers autorisés de leurs responsabilités.

En l'absence d'un tel accord cadre, les modalités de partage des renseignements devraient être stipulées dans une entente conclue entre le ministère fédéral d'origine et le gouvernement provincial ou le ministère concerné.

De telles ententes devraient inclure les éléments suivants :

- Une description générale des types de renseignements à partager.
- Les raisons pour lesquelles les renseignements sont partagés.
- Une stipulation selon laquelle ces renseignements ne doivent être communiqués qu'aux personnes qui en ont besoin au sein du ministère destinataire.
- Toutes les mesures de protection administratives, techniques et matérielles requises pour protéger les renseignements en cause.
- L'obligation pour le destinataire de dresser une liste de tous les fonctionnaires, par poste, qui auront accès aux renseignements.
- Les conditions de communication des renseignements aux tiers.
- Les noms, titres et signatures des fonctionnaires compétents du ministère d'origine et du gouvernement provincial destinataire, ainsi que la durée précise de l'entente.

Ces éléments sont évidemment pris en considération suivant le degré de préjudice qui pourrait résulter de l'atteinte à l'intégrité des renseignements.

Dans tous les cas, les conditions de communication à un tiers énoncées ci-dessus incluent l'obtention au préalable de l'autorisation du ministère fédéral d'origine. Une autre condition est que l'on doit respecter les conditions posées par le ministère d'origine lorsque les renseignements sont communiqués à un tiers. En outre, l'entente doit comporter un avis soulignant que le non-respect de cette condition mettra un terme au partage de ce type de renseignements.

Dans certaines circonstances, il peut arriver qu'on fournisse des renseignements confidentiels ou secrets à des organismes extérieurs sans exiger une cote de sécurité, par exemple pour des programmes approuvés par un administrateur général en vue de partager des renseignements classifiés avec des gouvernements provinciaux. Il ne faut en aucun cas fournir des renseignements très secrets avant que le destinataire ait reçu une cote de sécurité de niveau III.

Le chapitre 3-5 du volume « Protection des renseignements personnels » du Manuel du Conseil du Trésor indique quels doivent être les éléments des ententes sur le partage de renseignements personnels avec des gouvernements étrangers et des organisations internationales ou provinciales. Le paragraphe 8(2) de la Loi sur la protection des renseignements personnels impose des conditions particulières pour le partage de renseignements personnels. On traite de ces conditions à la section 6 du volume « Protection des renseignements personnels ». Les éléments des ententes peuvent toutefois être adaptés pour tenir compte des renseignements commerciaux de tiers, des renseignements des forces policières et autres, dans les cas qui ne relèvent pas de la Loi sur la protection des renseignements personnels.

14. Sécurité du télétravail

La politique gouvernementale sur le télétravail permet aux employés, avec l'accord de leur gestionnaire, de travailler loin de leur lieu de travail officiel. Pour de plus amples renseignements au sujet du travail à distance, voir la politique de télétravail, chapitre 2-4 du volume « Ressources humaines » du Manuel du Conseil du Trésor.

La politique de télétravail ne diminue en rien la responsabilité de protéger les renseignements et biens de nature délicate. Conséquemment, les agents de sécurité au nom de leur ministères devraient prendre les mesures qui s'imposent afin d'aviser et aider les gestionnaires et employés à minimiser les risques inhérents au fait d'enlever du lieu de travail les renseignements de nature délicate.

Compte tenu des risques élevés, le télétravail ne devrait pas impliquer l'accès aux renseignements désignés de nature extrêmement délicate ou classifiés très secret. Les politiques ministérielles devraient offrir des conseils quant à l'accès des employés aux autres renseignements de nature délicate pour leur travail à distance.

On devrait, dans le cadre de l'aide aux employés, faire des présentations sur certains aspects de la protection sure et le contrôle des renseignements de nature délicate et faire en sorte que ces employés puissent satisfaire à leurs obligations.

15. Formation de sensibilisation à la sécurité

Le programme de sensibilisation à la sécurité est un volet essentiel de tout programme complet et efficace sur la sécurité.

Le programme de sensibilisation à la sécurité qui comporte une série d'activités vise deux objectifs généraux :

- Assurer que tous les employés sont au courant de leurs responsabilités et de leur rôle concernant à la mise en œuvre et le maintien de la sécurité au sein du Ministère.
- Gagner et assurer la coopération du personnel en ce qui a trait à ces responsabilités et à ce rôle.

Le programme de sensibilisation à la sécurité attire l'attention sur la menace et expose en détail la politique et les procédures gouvernementales touchant la protection des renseignements et des biens du Ministère. Il convient de souligner aux employés, quel que soit leur niveau, que la sécurité fait partie de leurs responsabilités ordinaires et ne saurait être considérée comme une mesure occasionnelle et facultative ni comme étant la responsabilité d'un tiers.

Pour être efficace, cette formation doit continuellement être renforcée. Les bulletins ou notes au personnel ainsi que les conférences sur divers sujets reliés à la sécurité peuvent s'avérer de bons moyens pour faire circuler les règlements de façon périodique.

16. Inspections et enquêtes

16.1 Généralités

L'application des mesures de protection devrait faire partie intégrante des tâches d'administration et de supervision, en plus assortie d'inspections périodiques ou régulières des lieux ou des systèmes où des biens ou des renseignements de nature délicate sont traités ou conservés. Les inspections peuvent également être effectuées dans le cadre du contrôle de l'accès à des points de transition. Les inspections sécuritaires sont effectuées de façon systématique et aléatoire; elles ne visent pas des employés en particulier; par contre, les enquêtes de sécurité sont en rapport avec des événements précis et peuvent donc porter sur certains employés. À titre d'exemples d'activités d'inspection, citons les vérifications effectuées dans les bureaux durant les périodes d'accès limité, le contrôle au clavier des systèmes informatiques, la vérification de l'accès des utilisateurs au systèmes et de l'utilisation du système de télévision en circuit fermé. Les infractions à la sécurité devraient faire l'objet d'enquêtes en vue de prendre des mesures correctives et, éventuellement, de faire rapport aux autorités compétentes.

Les inspections devraient avoir lieu à la fin des heures de travail normales et être faites par le personnel ou les gardes de sécurité (s'il y en a), et au début et à la fin des périodes de travail par les personnes nommées à l'unité organisationnelle.

On devrait rapporter sans délai toute anomalie de la sécurité et toutes les infractions et manquements soupçonnés à la sécurité, et les mesures de redressements devraient être prises afin d'éviter que le problème continue.

16.2 Vie privée

La Charte canadienne des droits et libertés garantit aux fonctionnaires le droit d'avoir des attentes raisonnables quant à la protection des renseignements personnels et ce droit s'étend au lieu de travail. Les fonctionnaires sont également protégés par la Loi sur la protection des renseignements personnels. Toute inspection ou enquête de sécurité effectuée sur le lieu de travail, y compris les perquisitions et les saisies, doit respecter ce droit et tenir compte de la nécessité pour le Ministère d'assurer la supervision, le contrôle et la réalisation efficaces des activités sur le lieu de travail. Lorsqu'il y a déséquilibre et que la perquisition ou la saisie apparaît déraisonnable, les preuves recueillies peuvent être jugées inadmissibles par le tribunal. En outre, le Ministère peut être tenu responsable, au civil ou au pénal, de tout dommage qui en résulterait.

La définition de « raisonnable » dépend de la situation qui prévaut dans chaque cas et peut varier d'un ministère à un autre, selon notamment les responsabilités et les activités spécifiques, la nature du lieu de travail et l'objet de l'inspection ou de l'enquête. En cas de contestation, il revient au Ministère de démontrer que la perquisition ou la saisie était raisonnable. Une politique ministérielle de sécurité établissant clairement les conditions dans lesquelles on peut procéder à une perquisition ou à une saisie constitue une preuve importante en pareil cas.

16.3 Politiques et procédures

Les ministères qui effectuent des inspections et des enquêtes de sécurité doivent avoir une politique qui établit les conditions dans lesquelles celles-ci peuvent être effectuées. Les politiques et les procédures relatives aux inspections de sécurité doivent être claires, non équivoques et exhaustives; elles doivent être raisonnables compte tenu des circonstances et portées à l'attention des employés avant d'être mises en œuvre. Elles doivent également être en conformité avec le régime de négociations collectives ou avec les conventions collectives en vigueur.

Informer les employés des politiques et procédures d'inspection et d'enquête avant leur mise en œuvre signifie qu'il faut donner un préavis raisonnable au personnel en place et un avis quant à leur application ou au commencement de leur application dans le cas des nouveaux employés. Le cas échéant, on devrait obtenir l'assentiment des personnes concernées.

Il faut agir avec prudence lorsqu'une inspection tend à pouvoir être assimilée à une enquête criminelle. En d'autres mots, toute inspection doit respecter les conditions énoncées dans la politique du Ministère et ne saurait être utilisée pour contourner les procédures prévues au Code criminel. En particulier, les inspections ne devraient pas servir de prétexte pour effectuer une perquisition ou pour recueillir des preuves de délit criminel en l'absence de motifs raisonnables.

Les politiques devraient stipuler que les infractions à la sécurité doivent être déclarées sans délai et les procédures devraient décrire de quelle façon et à qui de tels rapports devraient être présentés.

On devrait en outre informer les employés de la raison d'être des politiques et procédures relatives aux inspections et aux enquêtes et chercher à obtenir leur coopération à ce chapitre.

Les politiques ministérielles relatives aux inspections et aux enquêtes devraient être examinées par les services juridiques du Ministère avant d'être mises en œuvre.

16.4 Infractions à la sécurité

Les ministères doivent établir des politiques et procédures à suivre en cas d'infraction à la sécurité. Ces procédures devraient comporter les points suivants :

- Signaler immédiatement les infractions présumées à la sécurité à l'administrateur général.
- Signaler immédiatement au SCRS toute divulgation présumée et non autorisée ou tout accès non autorisé aux renseignements ou biens classifiés.
- Signaler aux forces policières compétentes toutes les infractions présumées constituer des délits criminels.
- Le cas échéant, informer le ministère d'où provenaient les renseignements et autres biens qu'il y a eu infraction à la sécurité.
- Informer les autres ministères dont les renseignements ou biens ont fait l'objet d'une infraction à la sécurité, des circonstances et des conclusions qui les concernent.
- Évaluer le préjudice dans les dix jours ouvrables lorsqu'il est probable qu'il y ait eu infraction à la sécurité et en faire rapport à l'administrateur général.

Cette obligation ne s'applique pas aux incidents mineurs; dans chaque cas, on doit tenir compte du préjudice possible à l'intérêt national. Les rapports devraient être acheminés par l'agent de sécurité du ministère. Pour faire rapport d'infractions présumées au SCRS, utilisez les adresses et numéros de téléphone de l'appendice A.

16.5 Délits criminels

Dans les cas soupçonnés de vol, fraude, détournement de fonds ou toute autre offense ou geste illégal impliquant les employés et n'exigeant pas une réponse policière immédiate, on peut se référer aux services juridiques ministériels afin d'obtenir une opinion quant à la gravité de l'incident avant de poursuivre. Sinon, toutes les pertes d'argent et tous les cas soupçonnés de fraude, de détournement de fonds ou toute autre offense ou geste illégal contre la Couronne doivent être rapportés aux autorités policières. Pour de plus amples renseignements, voir le chapitre 8 du volume « Gestion financière » du Manuel du Conseil du Trésor.

16.6 Fouilles lors d'enquêtes criminelles

L'agent de sécurité du ministère en consultation avec le personnel juridique du ministère et les autorités policières locales doit revoir les obligations de fouiller dans le cadre d'une enquête au sujet d'un délit soupçonné ou potentiel de nature criminelle. Il faut obtenir un mandat à chaque fois que la loi le requiert.

16.7 Communication de renseignements de nature délicate

Il se peut, parfois, que les enquêteurs et d'autres personnes non autorisées à avoir accès à des renseignements de nature délicate soient mis en présence de tels renseignements durant leur fouille. Dans ce cas, l'agent de sécurité du ministère en consultation avec le gestionnaire, doit revoir le préjudice possible aux renseignements et agir en tenant compte des intérêts tant de l'enquête que de l'intention de la Politique sur la sécurité.

Les faits précédents impliquent des difficultés pouvant nécessiter un statut spécial d'enquête de sécurité, une consultation juridique et des pouvoirs exécutifs afin de les résoudre.

16.8 Preuves

Dans tous les cas où des renseignements de nature délicate risquent de faire l'objet d'un examen public minutieux dans le cadre d'un acte judiciaire, l'agent ministériel de sécurité doit consulter les services juridiques du Ministère.

Le personnel du Ministère susceptible d'être appelé à témoigner ou à fournir des preuves dans le cadre de poursuites judiciaires liées à une infraction criminelle devrait consigner par écrit ces démarches afin de pouvoir étayer les preuves qu'il pourrait être appelé à donner.

16.9 Collaboration aux fins d'une enquête

Il est souvent nécessaire pour les ministères, la police ou d'autres organismes de coopérer pour pouvoir effectuer une enquête intégrale et exhaustive. Le cas échéant, des protocoles devraient être établis pour réglementer les exigences relativement à la coopération et les ministères devraient les inclure dans leurs politiques et procédures. Toutefois, ces protocoles, politiques et procédures ne sauraient être utilisés pour contourner l'obligation d'avoir un mandat ou toute autre obligation constitutionnelle.

16.10 Tests des systèmes de sécurité

On devrait tester périodiquement les procédures, les plans et le matériel de sécurité, mais en tenant compte des conséquences négatives possibles que des réactions inappropriées pourraient avoir. De tels tests pourraient inclure l'entrée dans une section contrôlée par un système d'alarme ou une zone de sécurité afin d'en vérifier les dispositifs de contrôle électronique.

On devrait aviser le personnel de surveillance des tests et évaluations planifiés qui pourraient affecter les mesures de sécurité.

On devrait considérer la possibilité d'utiliser des exercices de perfectionnement, élaborés et employés pour évaluer les capacités en termes de sécurité et les niveaux de connaissances et de sensibilisation des employés, lorsque des incidents laissent croire qu'il existe certaines faiblesses, ou lorsqu'on veut renforcer l'efficacité du programme de sécurité.

17. Gestion des gardes de sécurité

Les ministères sont chargés de déterminer leurs exigences et les fonds pour les gardes de sécurité devant protéger les renseignements et les biens.

Les ministères gardiens sont chargés d'offrir et de trouver les fonds pour les gardes devant protéger les installations à la suite d'une évaluation de la menace et des risques, et sur des sites précis.

On devrait essayer de réduire les coûts des gardes en aménageant de façon efficace les nouveaux édifices et la disposition des étages ainsi qu'en utilisant d'autres méthodes de protection.

En vertu des exigences de la Politique sur la sécurité les gardes devront faire l'objet d'une enquête de sécurité adéquate, compte tenu de leur accès possible aux renseignements et aux biens de nature délicate. Cela ne comprend pas les situations où l'accès découle de la découverte d'une infraction à la sécurité.

Travaux Publics et Services gouvernementaux Canada est chargé d'offrir des conseils et des avis quant aux enquêtes de sécurité et à l'embauche des gardes.

Vous trouverez en appendice B une liste de documents de références.

Appendice A - Conseils

Généralités

Toute demande de renseignements devrait être adressée aux agents responsables des administrations centrales qui, à leur tour, pourront obtenir des interprétations auprès de la Division de la sécurité et gestion de l'identité.

Source de renseignements au sujet des évaluations de la menace

Pour les évaluations de menaces d'espionnage, de sabotage ou de terrorisme à l'endroit des renseignements et biens ministériels, telles que décrites à l'article 2 de la Loi sur le SCRS, vous pouvez vous adresser au :

Directeur adjoint
Direction des analyses et productions
Service canadien du renseignement de sécurité
C.P. 9732
Station T
Ottawa (Ontario)
K1G 4G4

Téléphone : 613-782-0243
(service jour et nuit)

Pour obtenir des renseignements et conseils sur les évaluations de risques et menaces en matières criminelles, de sécurité matérielle, et aspects généraux de la sécurité des technologies de l'information, vous pouvez vous adresser à :

Agent responsible
Systèmes de sécurité
GRC
1200, Promenade Vanier
Ottawa (Ontario)
K1A 0R2
Téléphone : 613-993-7977
Télécopieur : 613-952-5512

Pour obtenir des renseignements sur les menaces techniques à la COMSEC et autres aspects pertinents de la sécurité des technologies de l'information, vous pouvez vous adresser à :

Chef
TRANSEC et soutien opérationnel
Centre de la sécurité des télécommunications
C.P. 9703
Terminus postal d'Ottawa

Ottawa (Ontario)
K1G 3Z4
Téléphone : 613-991-7482

Appendice B - Références

- Volume « Perspective des renseignements personnels », Manuel du Conseil du Trésor
- Pratiques administratives : Lignes directrices à l'intention des Cabinets des ministres, Secrétariat du Conseil du Trésor
- Guide de la gestion des services d'agents de sécurité (DSS/GS-29) Gendarmerie royale du Canada, 1993
- Volume « Gestion de l'information », Manuel du Conseil du Trésor
- Volume « Gestion des risques, des services et du matériel », Manuel du Conseil du Trésor
- Volume « Protection des renseignements personnels », Manuel du Conseil du Trésor
- Agents de sécurité en uniforme (CAN/CGSB133.1-87), Office des normes générales du Canada
- Superviseur des agents de sécurité en uniforme (CAN/CGSB133.2-92), Office des normes générales du Canada
- Politique de télétravail, chapitre 2-4, volume « Ressources humaines », Manuel du Conseil du Trésor
- Services de sécurité « Commissionnaires et autres gardes, chapitre 370, Manuel du client (Gestion du matériel), Services gouvernementaux Canada

Appendice C - La classification des renseignements touchant l'intérêt national

Traditionnellement, la sécurité administrative au sein du gouvernement du Canada a reposé sur le système de classification des renseignements et des biens de nature délicate. Ce système a été mal utilisé lorsqu'on a classifié des renseignements autres que ceux se rapportant à l'intérêt national, et cela a diminué l'efficacité des moyens de protection des renseignements gouvernementaux de nature délicate et a conduit à des moyens de protection injustifiés dont l'enquête de sécurité sur les individus. En classifiant les renseignements, les ministères doivent s'assurer de peser le risque de préjudice à l'intérêt national par rapport à ce qu'il en coûte de protéger des renseignements ayant des classifications très élevées.

Il n'y a que peu de renseignements dans les ministères qui exigent une classification dans l'intérêt national. On doit surveiller de près le seuil qui, une fois franchi, causerait un préjudice à l'intérêt national et le circonscrire afin d'éviter toute dilution pouvant saper la crédibilité de l'ensemble du système de classification. Ce qui compte est le contenu du dossier, la substance des renseignements. Les conseils suivants offrent une base pour déterminer quand les renseignements se rangent dans la catégorie de l'intérêt national.

Les affaires fédérales-provinciales (s. 14, LAI)

S'entend des renseignements lorsqu'une atteinte à leur intégrité pourrait vraisemblablement porter préjudice à la conduite par l'administration fédérale des affaires fédérales-provinciales. L'exemption n'a pour but que de préserver le rôle de l'administration fédérale et non l'ensemble des relations fédérales-provinciales. Normalement, ceci touchera aux consultations et aux délibérations fédérales-provinciales et aux stratégies et tactiques adoptées pour la conduite des affaires fédérales-provinciales au nom de l'ensemble du gouvernement lorsqu'on considère les divisions de pouvoirs et les formes de gouvernement. (par exemple, les négociations constitutionnelles).

La catégorie ne couvre pas l'infinité d'activités fédérales-provinciales poursuivies par la majorité des institutions fédérales. Celles-ci peuvent peut-être faire exception à l'accès en vertu de la Loi sur l'accès à l'information mais la catégorie désignée offre une protection adéquate.

Affaires internationales et défense (s. 15, LAI)

S'entend des renseignements lorsqu'une atteinte à leur intégrité pourrait vraisemblablement porter préjudice à la conduite des affaires internationales, à la défense du Canada ou de tout autre État allié ou associé au Canada ou à la détection, la prévention ou à la répression d'activités hostiles ou subversives. Cette catégorie comprend les questions traditionnelles de sécurité nationale où la divulgation de renseignements porterait préjudice à la sécurité de la nation. Les exemples de documents de ce type sont :

- Les planifications et négociations diplomatiques dont le but principal est le maintien de la sécurité de la nation.
- Les aspects de processus de négociations (par exemple, la stratégie, les tactiques, et les positions) pouvant donner un avantage injuste à une autre nation.
- Les analyses ou commentaires sur les affaires internes d'une autre nation qui, divulgués, ne seraient pas dans l'intérêt du Canada.
- La correspondance diplomatique échangée avec des pays étrangers ou organismes internationaux d'États, ou la correspondance officielle échangée avec les missions diplomatiques ou consulats canadiens à l'étranger. Il est fort possible que la plupart de la correspondance officielle ne soit pas classifiée telle la correspondance au sujet de l'administration interne des missions et les programmes culturels et d'information publique.
- Les plans de défense tactique et stratégique, les opérations ou exercices, comprenant les spécifications de l'équipement, des techniques militaires et leur taille, leur mouvement et l'emplacement des forces.
- Les renseignements obtenus ou préparés dans le but de se renseigner quant à la défense ou la détection, la prévention ou la suppression d'activités hostiles ou subversives. Ceci comprend tant les données bruts (renseignements obtenus) que le produit raffiné ou l'analyse (renseignements préparés).
- Les méthodes, l'équipement technique ou scientifique pour recueillir, évaluer ou traiter les renseignements au sujet des relations internationales, la défense, la sécurité et les renseignements.
- Les communications ou systèmes cryptographiques du Canada ou de pays étrangers utilisés dans les affaires internationales, la défense du Canada ou d'États alliés ou associés au Canada, ou pour la détection, la prévention ou la suppression

d'activités hostiles ou subversives.
- Les enquêtes licites sur des activités soupçonnées de menacer la sécurité du Canada au sens de la Loi sur le Service canadien du renseignement de sécurité et les techniques d'enquêtes ou des projets pour de telles enquêtes.

Étant donné la nature des renseignements, on les trouverait normalement au bureau du Conseil Privé, aux Affaires étrangères et Commerce international, au ministère de la Défense nationale et dans les agences nationales de sécurité et de renseignements.

Les enquêtes sur la sécurité du Canada (al. 16(1)a)(iii), 16(1)b) et 16(1)c) LAI)

Les renseignements de cette catégorie pouvant être classifiés sont très restrictifs puisque les renseignements doivent concerner des menaces à la sécurité du Canada telles que décrites à la section 2 de la Loi sur le Service canadien du renseignement de sécurité. Très peu de ministères, sauf principalement le SCRS et la GRC, gardent de tels renseignements.

Pour être classifié, les renseignements doivent :

- Avoir été obtenus ou préparés par les organismes d'enquête fort peu nombreux et décrits dans les règlements découlant des lois sur l'accès à l'information ou la protection des renseignements personnels.
- Avoir été obtenus ou préparés au cours d'une enquête licite.
- Concerner des activités soupçonnées de menacer la sécurité du Canada au sens de la Loi sur le Service canadien du renseignement de sécurité.

Les renseignements concernant les techniques d'enquêtes ou des projets d'enquêtes licites déterminées ayant un rapport avec ce qui précède pourraient aussi être classifié dans l'intérêt national.

Les intérêts économiques du Canada (al. 18a) et d), LAI)

Cette section compte deux parties. La première se réfère aux secrets industriels, ou aux renseignements financiers, commerciaux, scientifiques ou techniques appartenant à l'administration fédérale ou à une institution gouvernementale, et a ou peut avoir une grande valeur. Certains renseignements et certaines technologies se rapportant aux armes nucléaires, biologiques ou chimiques se doivent d'être classifiés. De même, certains domaines de recherche en technologie de pointe et sciences spécialisées tels que les communications avancées, l'électronique, la technologie et la biotechnologie chimique, comprenant les applications militaires peuvent devoir être protégés dans l'intérêt national.

On doit noter, toutefois, que ce n'est qu'une partie de l'ensemble des recherches scientifiques et techniques du gouvernement puisque le but de la plus grande partie des recherches est de promouvoir le développement industriel national et la compétitivité économique. Souvent la recherche et le développement se font en partenariat avec le secteur privé et les renseignements relèvent surtout du domaine public. Exception faite des renseignements qui peuvent devoir être classifiés, les autres renseignements de nature délicate sont protégés de façon adéquate en termes de matériel désigné.

La deuxième partie se réfère aux renseignements qui, si divulgués, pourraient raisonnablement porter préjudice matériel aux intérêts financiers de l'administration fédérale et à sa capacité de gérer l'économie. On trouve des exemples dans les renseignements se rapportant :

- À la devise, au système monétaire ou au cours légal du Canada.
- Aux changements envisagés des tarifs, des impôts, des droits de douane ou d'autres sources de revenus.
- Aux changements envisagés aux modes d'opérations des organismes financiers.

À la vente ou à l'achat envisagé de titres ou de devises canadiennes ou étrangères.

Cette catégorie a pour but d'englober la gestion de l'économie nationale. Ce type de renseignements se trouve normalement au ministère des Finances, à la Banque du Canada et au ministère du Revenu.

Appendice D - Le marquage des renseignements de nature délicate

Voici des suggestions de procédures pour le marquage et le contrôle des renseignements de nature délicate.

Renseignements très secrets

Inscrire dans le coin supérieur droit de chaque page la mention Très SECRET et le nombre total de pages. Assigner un nombre unique a chaque exemplaire en inscrivant le numéro de l'exemplaire sur chaque page, et tenir à jour une liste de distribution. On devrait faire des copies supplémentaires des renseignements de nature délicate seulement si le détenteur de l'original assigne une identification unique a chaque exemplaire produit ultérieurement et tient à jour une liste de distribution.

Renseignements secrets

Inscrire la mention SECRET sur chaque page du document, dans le coin supérieur droit. Numéroter chaque exemplaire sur le verso de la page et tenir à jour une liste de distribution.

Renseignements confidentiels

Inscrire la mention CONFIDENTIEL dans le coin supérieur droit de la première page du document. Contrôler le nombre de copies de documents confidentiels de la même façon que pour les documents secrets, lorsque l'évolution de la menace et des risques justifie

cette mesure.

Renseignements désignés.

Sous réserve d'exceptions discrétionnaires, inscrire la mention PROTEGE dans le coin supérieur droit de la première page du document. De plus, on peut préciser pourquoi les renseignements sont de nature délicate ou quelles mesures de protection sont nécessaires. On peut utiliser les lettres suivantes pour signaler les mesures de protection appropriées en ce qui concerne les renseignements désignés : « A » pour nature peu délicate; « B » pour nature particulierement delicate et « C » pour nature extrememement delicate.

Généralités

- Inscrire la mention sur les pages couvertures, les lettres d'introduction, les formulaires ou les bordereaux d'acheminement la classification de sécurité ou la désignation la plus élevée des pièces jointes.
- Inscrire la mention sur tout ce qui a servi à préparer des renseignements classifies ou désignés. Il peut s'agir de notes, d'ébauches, de copies au carbone ou de photocopies.
- Le marquage peut également spécifier qui peut ou non avoir accès aux renseignements afin de limiter d'avantage l'accès a ceux-ci.
- Le marquage de sécurité devrait inclure la classification ou la désignation applicable et la date ou l'événement a la suite duquel se produira la déclassification ou le déclassement; il faudrait, dans la mesure du possible déterminer ces données au moment ou les renseignements sont crées ou recueillis.
- Assigner la classification ou la désignation de sécurité la plus élevée ou la désignation des renseignements comprise sur la microforme.
- Inscrire la mention sous une forme qui peut être lue, sur les microformes renfermant des informations classifiées, la classification appropriée de même que le numéro de la microforme et le nombre total de celles-ci;
- Inscrire la mention PROTEGE, sous une forme qui peut être lue, de même que le numéro de la microforme et le nombre total de microformes.

Sécurité

Pour plus de renseignements au sujet du marquage des supports électroniques de stockage, voir le document intitule *Normes techniques de sécurité pour les technologies de l'information* qui figure à l'appendice A, au chapitre 2-3.