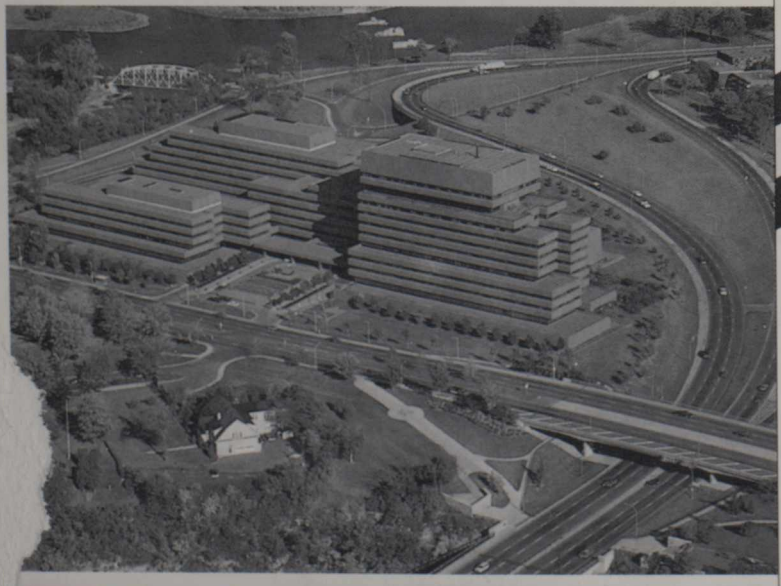
LA SÉCURITÉ À L'ADMINISTRATION CENTRALE

...Guide de l'employé



Affaires extérieures et Commerce extérieur Canada

Canada

Table des matières

1. Introduction

Le présent guide est publié par l'Agent de sécurité du Ministère (ISS).

Vous y trouverez un résumé et une explication des principales dispositions des politiques de sécurité du Ministère applicables à l'Administration centrale. À ce titre, le guide ne saurait remplacer les politiques elles-mêmes. Pour de plus amples renseignements, veuillez consulter le *Manuel des instructions de sécurité* ou la section appropriée de ISS, soit ISSG dans la plupart des cas.

Certains aspects des dispositions sur la sécurité physique et des mesures d'urgence s'appliquent spécifiquement à l'édifice Lester B. Pearson. Les employés du Ministère et le personnel sous contrat qui travaillent dans d'autres immeubles à Ottawa ou ailleurs au Canada (les sites de conférences compris), doivent respecter les dispositions sur la sécurité et les mesures d'urgence qui prévalent aux endroits concernés.

2. Sécurité physique

Zones et secteurs de sécurité

Le système de sécurité du Ministère divise l'édifice Lester B. Pearson en un certain nombre de zones de sécurité, dans le but d'en contrôler l'accès et de protéger tous les biens du gouvernement contre les pertes, les dommages, les vols et la divulgation.

Zone publique

Le rez-de-chaussée de l'édifice est ouvert au public. Dans cette zone se trouvent la bibliothèque du Ministère, la cafétéria, la Banque Royale du Canada, l'auditorium, la salle de conférences principale et le hall d'entrée.

Secteur à accès réglementé

Les quatre tours sont désignées « secteur à accès réglementé », et l'accès en est contrôlé par des membres du Corps canadien des commissionnaires. Seules les personnes munies d'un laissez-passer approprié ou les **visiteurs escortés** peuvent y entrer.

Zone de sécurité

À l'intérieur des secteurs à accès réglementé se trouvent des zones de sécurité auxquelles seules les personnes autorisées ont accès. L'accès à une partie, mais non à la totalité, des zones de sécurité est restreint encore davantage par des portes munies de serrures à combinaisons de sûreté et d'autres dispositifs.

Indications d'accès restreint

À l'intérieur des secteurs à accès réglementé, des indications telles que « zone de sécurité » sont utilisées pour identifier les secteurs ou zones très protégées ou sensibles. Des indications additionnelles telles que « Réservé au personnel autorisé » peuvent être utilisées. Seules les personnes ayant affaire dans ces endroits pour leur travail sont autorisées à y entrer.

Zone de réception (Tour A)

Le 9e étage de la Tour "A" est une zone de réception où se tiennent des fonctions ministérielles à l'intention des visiteurs. Étant donné qu'ils

doivent passer dans le secteur à accès réglementé de la Tour A, les visiteurs doivent être escortés comme il convient pour se rendre à l'étage et pour en revenir; ils ne doivent pas pouvoir accéder seuls à d'autres étages de la Tour A.

Contrôle de l'entrée et de la sortie

Laissez-passer

ISSG délivre des laissez-passer pour contrôler l'accès aux quatre tours de l'édifice Lester B. Pearson. On ne délivre de laissez-passer aux employés du ministère et au personnel désigné que lorsque ISSV leur a accordé une autorisation de sécurité. Le titulaire doit rendre son laissez-passer à ISSG au moment de sa mutation ou à la fin de son emploi. On doit signaler la perte de son laissez-passer à l'agent des opérations de sécurité dès qu'on s'en rend compte.

Accès en dehors des heures de travail

Les employés doivent posséder un laissez-passer valide du Ministère et signer un registre d'entrée/sortie afin de pouvoir accéder aux installations du Ministère après les heures normales de travail, soit après 18h les jours ouvrables, et toute la journée les samedis, dimanches et jours fériés.

Permis de stationnement

Les permis de stationnement sont délivrés par MFM et toute question à ce sujet devrait être adressée à cette direction. Grâce à une entente spéciale avec la GRC, ISSG se charge de faire respecter les règlements établis par la *Loi relative à la circulation sur les terrains de l'État.*

Corps canadien des commissionnaires

Les membres du Corps canadien des commissionnaires contrôlent l'accès à l'immeuble et accompagnent tous les visiteurs. Ces derniers sont escortés jusqu'au bureau de l'employé qu'ils désirent rencontrer et il appartient à celui-ci de les raccompagner jusqu'au hall d'entrée principal à la fin de la rencontre.

Visiteurs – Responsabilité des employés

Les personnes qui n'ont pas de laissez-passer doivent être escortées en tout temps dans les secteurs à accès réglementé et les zones de sécurité de l'édifice Lester B. Pearson. Les visiteurs et les techniciens à l'entretien de l'équipement qui ont rendez-vous avec des employés du Ministère sont accompagnés par le Service d'escorte des visiteurs de ISS ou par un employé jusqu'au bureau ou au poste de travail de la personne en question. Le visiteur **doit** aussi être raccompagné jusqu'au hall d'entrée principal lorsque son travail est terminé. Cette mesure de sécurité est nécessaire pour empêcher les visiteurs de circuler librement dans l'immeuble et d'entrer dans des secteurs où se déroulent des opérations ou des entretiens de nature délicate.

Ceux qui se dérobent à cette responsabilité commettent une infraction à la sécurité.

Responsabilité des employés en dehors des heures normales de travail

Il arrive souvent que des employés demeurent au bureau après les heures normales de travail pratiquées à Ottawa. Même si l'édifice est sous la surveillance du personnel de sécurité de ISS pendant ces heures, il est dans l'intérêt des employés d'informer le personnel de sécurité de leur présence, comme l'exige le Code du travail du Canada, au cas où se produirait une situation d'urgence.

Les employés qui demeurent dans l'immeuble en dehors des heures de travail doivent en informer l'agent de sécurité au bureau de réception (entrée principale) en composant le 995-5859.

Serrures et combinaisons

Cadenas à combinaison S & G

Chaque employé est responsable de la protection du matériel classifié en sa possession. On peut obtenir des cadenas à combinaison S & G approuvés en téléphonant au 992-6679 (ISSG).

Changement des combinaisons

Il faut accorder à la combinaison d'un cadenas la même protection qu'au matériel classifié qu'elle protège. Elle devrait être changée tous les six mois, lorsqu'une personne la connaissant est mutée ou n'a plus

besoin d'accéder aux contenants de sécurité, et lorsque la combinaison a été ou pourrait avoir été divulguée.

Clés des bureaux

Les clés des bureaux doivent être protégées et il ne faut pas les reproduire; les clés excédentaires devraient être sous le contrôle des secrétaires de direction. On peut obtenir de nouvelles clés ou de nouvelles serrures en téléphonant au 992-6679 (ISSG).

La négligence en matière de protection des clés constitue une infraction à la sécurité.

Protection des effets personnels et des biens de l'État

Procédures

Il appartient aux employés de protéger leurs effets personnels. Les sacs à main, les portefeuilles et l'argent devraient être gardés avec soi ou protégés en tout temps et les articles ayant une valeur sentimentale devraient être mis sous clé en dehors des heures de travail.

Les employés ont aussi la responsabilité de ranger, dans des armoires ou des pièces fermées à clé, les articles tentants qui appartiennent à l'État – calculatrices, ordinateurs, magnétophones, appareils photo, etc., – lorsqu'ils ne sont pas utilisés.

Objets perdus et volés

Il faut alerter la Direction de la sécurité (ISSG, 996-4731) dès que des objets ont été perdus ou volés. Étant informés immédiatement, les agents de sécurité peuvent plus facilement mener leur enquête.

3. Mesures d'urgence

Exigences

La Partie XVII du *Règlement du Canada sur l'hygiène et la sécurité au travail* établi en vertu du *Code canadien du travail* prévoit la mise sur pied d'une organisation de secours en cas d'incendie dans tous les immeubles occupés par le gouvernement du Canada. L'organisation est en fonction pendant les heures de travail. Sur chaque étage, des bénévoles font des vérifications de sécurité en plus de ses tâches ordinaires.

Responsabilités

ISSG est responsable de l'élaboration et de la mise en oeuvre des procédures, règlements et instructions se rapportant aux incendies et à d'autres cas d'urgence où la sécurité du personnel est menacée. En outre, cette section s'occupe de la formation de tous les employés et supervise l'évacuation de l'immeuble dans les cas d'urgence.

Formation

Les membres de l'Organisation de secours ont reçu une formation dans les domaines suivants :

- Premiers soins
- Mesures d'urgence en cas d'incendie
- Utilisation des extincteurs
- Mesures d'urgence en cas de menaces
- Mesures d'évacuation

Mesures d'urgence de l'édifice

Des mesures d'urgence ont été établies pour l'édifice Lester B. Pearson et distribuées à toutes les directions. Elles ont été approuvées par le Directeur de la sécurité et les présidents du Comité de sécurité et d'hygiène au travail de l'édifice.

Ces mesures ont été conçues pour permettre de répondre rapidement et efficacement à une grande variété de situations d'urgence susceptibles de se produire à l'édifice Lester B. Pearson. Il peut s'agir d'une alerte d'incendie, d'une urgence d'ordre médical, d'une menace à la sécurité ou d'une panne importante de l'équipement de l'immeuble; en bref, des situations qui exigent l'intervention des services de secours de l'édifice ou des services de secours municipaux.

L'expérience montre que, dans des situations d'urgence, la plupart des gens réagissent d'une manière raisonnable, mais pas nécessairement de la même façon. Par conséquent, l'établissement de mesures d'urgence simples, comprises et pratiquées par les organismes d'urgence et par les occupants, constitue le meilleur moyen d'assurer une réponse coordonnée et efficace à une situation donnée. Les occupants de l'édifice devraient prendre le temps de les lire, afin que nous puissions tous agir ensemble de la manière la plus sûre possible en cas d'urgence.

Les mesures d'urgence établies pour l'édifice ne doivent pas être confondues avec les plans et procédures du Ministère concernant les opérations d'urgence et la gestion des crises. Dans certaines circonstances, le recours à ces plans et procédures pourrait s'avérer nécessaire, par exemple lorsqu'un problème concernant l'édifice risque de nuire sérieusement au fonctionnement du Ministère, qu'un incident destructeur comme un incendie exige qu'on établisse un plan de « recouvrement », ou que l'incident est de nature régionale, nationale ou internationale.

Les priorités des plans de secours de l'édifice sont les suivantes :

1. la sécurité de tous les occupants;

2. la protection et la préservation de l'information, des systèmes et des opérations jugés d'une importance capitale pour l'accomplissement du mandat du Ministère; et

3. la protection des autres opérations et des biens privés et ministériels.

Centre de contrôle des mesures d'urgence de l'édifice Pearson

Pour la plupart des cas d'urgence, c'est là qu'il faut appeler d'abord. Il peut s'agir :

d'un incendie – évacuation
d'une urgence d'ordre médical – ambulance, unité de la santé, premiers soins
d'une menace à la bombe – téléphone, colis
d'actes criminels, de nuisance publique, d'intrusions – police et services de sécurité
de pannes des systèmes de l'édifice – équipement, services publics
de sinistres – avertissements, mesures à prendre, organisations

Selon le cas, utilisez les téléphones rouges, composez le 992-1150 au moyen d'un téléphone ordinaire, ou tirez la manette d'alarme.

Le centre de contrôle, situé au rez-de-chaussée de la Tour B, fonctionne 24 heures par jour et compte un personnel bilingue bien formé, faisant partie du Corps canadien des commissionnaires, qui connaît tous les aspects de l'édifice. Ces personnes peuvent communiquer par radio avec toutes les parties de l'édifice pendant les heures normales de travail et avec certaines parties en dehors des heures de travail. Le centre fait la vérification des systèmes d'alarme de l'édifice et du système de téléphones rouges qui compte plus d'une centaine d'appareils. Tous les plans d'étage et un jeu complet de clés y sont conservés pour prêter main-forte au Service d'incendie d'Ottawa lorsqu'il répond à une alerte.

Sur réception d'un message d'urgence, le centre de contrôle communiquera avec tous les services d'urgence :

— les services d'urgence municipaux et régionaux
— d'autres services d'urgence externes
— les services d'urgence de l'édifice Pearson
— l'organisation des services de secours de l'édifice

Agents des services de secours d'étage

Un agent principal des services de secours est nommé pour chaque étage de chaque tour.

Un agent des services de secours est nommé pour chaque aire de travail de chaque étage.

Personnes souffrant de perte de mobilité

Les personnes qui souffrent d'une perte de mobilité ou d'acuité sensorielle de même que celles qui sont temporairement handicapées à la suite d'une blessure ou d'un problème de santé sont priées de s'identifier auprès des personnes qui acceptent de devenir leur moniteur personnel, de l'agent de secours d'étage de leur aire de travail et du Centre de contrôle d'urgence. En cas d'urgence, ce dernier et le Service d'incendie d'Ottawa, étant ainsi renseignés, pourront maîtriser la situation en toute sécurité. Par contre, si la personne souffrant d'un malaise quelconque ne veut pas révéler son état, elle devrait au moins avertir l'agent de secours d'étage aussitôt que l'alarme sonne.

4. Classification de l'information à des fins de sécurité

Que faut-il protéger?

L'information et les biens qui appartiennent au Ministère devraient, à tout le moins, recevoir la protection généralement associée à de saines pratiques de gestion.

Toutefois, certains renseignements et biens sont de nature plus délicate ou ont une plus grande valeur que les autres et doivent par conséquent être mieux protégés. Conformément aux dispositions de la *Loi sur l'accès à l'information,* de la *Loi sur la protection des renseignements personnels,* et de la politique du gouvernement sur la sécurité, le Ministère a divisé son matériel d'information en trois catégories :

- le matériel qui porte sur la sécurité nationale
- le matériel se situant à l'extérieur des paramètres de l'intérêt national, mais qui est néanmoins de nature délicate ou de grande valeur
- le reste du matériel qui n'est pas nécessairement entièrement du domaine public

Si l'on peut raisonnablement prévoir que l'information sera exemptée de divulgation en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels,* il faut lui assigner soit une cote de classification, soit une désignation.

Les biens matériels qui touchent à l'intérêt national ainsi que d'autres biens de nature délicate ou ayant une certaine valeur exigent également une protection particulière. Citons, par exemple, tout le matériel informatique du système COSICS.

L'information reçue confidentiellement d'autres gouvernements doit être traitée conformément aux accords ou ententes négociés avec eux.

Information classifiée dans l'intérêt national

La politique du gouvernement sur la sécurité prévoit que l'information doit être classifiée s'il est raisonnable de croire que sa divulgation sans autorisation irait à l'encontre de l'intérêt national. Aux fins de la politique sur la sécurité, « l'intérêt national » englobe « la stabilité sociale, économique et politique du Canada et, par extension, la sécurité du pays ». D'une manière générale, les exceptions prévues par les lois

sur l'accès à l'information et sur la protection des renseignements personnels qualifient de délicates dans l'intérêt national les informations qui concernent :

- les relations fédérales-provinciales, les affaires internationales, la défense ou les intérêts économiques du Canada
- les avis et recommandations portant sur les points susmentionnés
- la sécurité et le renseignement, ou le processus d'établissement des autorisations personnelles.

Une information ne devrait jamais être classifiée dans l'intérêt national pour dissimuler des violations de la loi, des lacunes ou des erreurs administratives, ou pour éviter des embarras ou réduire la concurrence.

Information désignée PROTÉGÉ (DÉLICAT)

Les lois susmentionnées interdisent la divulgation de certaines informations parce qu'elles seraient préjudiciables à des intérêts spécifiques, publics ou privés. Ces informations doivent porter la cote PROTÉGÉ (DÉLICAT) s'il est raisonnable de croire qu'elles feraient l'objet d'exceptions aux termes des lois susmentionnées parce qu'elles concernent :

- des enquêtes policières
- la sécurité de particuliers
- la position concurrentielle du gouvernement
- les activités de recherche, des méthodes d'essai et des vérifications
- des renseignements commerciaux appartenant à une tierce partie
- le secret professionnel de l'avocat
- d'autres paliers de gouvernement (renseignements obtenus sous le sceau confidentiel)
- des dossiers médicaux
- des personnes particulières ou des employés fédéraux
- des questions dont d'autres lois (p. ex. la *Loi sur la statistique)* interdisent la divulgation

Information désignée PROTÉGÉ – PERSONNEL

La politique du gouvernement sur la sécurité précise que les renseignements personnels doivent faire l'objet d'une protection particulière.

Certains renseignements concernant les employés du Ministère sont de nature délicate et doivent être protégés de façon spéciale, par exemple :

- les salaires (sauf l'échelle des salaires)
- les évaluations de rendement
- les dossiers médicaux
- les déclarations de conflit d'intérêts

Les avis reçus à propos de renseignements de nature délicate doivent aussi être évalués quant aux effets néfastes d'une divulgation éventuelle. Il peut être indiqué de leur assigner une désignation.

> N'oubliez pas qu'il est extrêmement important de protéger aussi les avis donnés dans le cadre d'un processus décisionnel qui touche directement une personne.

Biens matériels

Certains équipements ou articles sont essentiels à la sécurité de l'information classifiée. On peut obtenir auprès d'ISSG des conseils sur la façon de les identifier et de les protéger. Tout l'équipement servant au COSICS ainsi qu'un grand nombre de machines à écrire, de machines de traitement de texte et de micro-ordinateurs font partie de cette catégorie d'équipement.

Les biens négociables, les machines de valeur, ou l'équipement essentiel à une fonction du Ministère doivent être désignés « de grande valeur » ou « de nature délicate ». On peut obtenir auprès d'ISSG des directives sur la façon de protéger les biens désignés.

Classification et désignation

Niveaux de classification et de désignation

Les trois niveaux de classification sont les suivants :

TRÈS SECRET:	Lorsqu'il est raisonnable de croire que les renseignements compromis pourraient porter un préjudice exceptionnellement grave à l'intérêt national. Dans ce contexte, compromis signifie divulgué, détruit, modifié, enlevé ou interrompu. Les effets doivent être considérables, immédiats et irréparables. Évidemment, le nombre de documents qui mérite cette cote de classification est très limité.
SECRET :	Lorsqu'on peut raisonnablement croire que les renseignements compromis pourraient porter un préjudice grave à l'intérêt national.
CONFIDENTIEL :	Lorsqu'on peut raisonnablement croire que les documents compromis pourraient porter préjudice à l'intérêt national. Il est clair que la plupart des renseignements ou des biens qui justifient une classification tombent dans cette catégorie.

Le gouvernement canadien n'emploie pas la classification DIFFUSION RESTREINTE. Toutefois, l'expression est utilisée pour l'information émanant de l'OTAN ou de l'OCDE (Organisation pour la coopération et le développement économiques). Cette information doit être traitée comme celle qui porte la cote PROTÉGÉ.

Les renseignements classifiés doivent porter la cote de sécurité appropriée au moment où ils sont produits ou recueillis.

Il y a deux niveaux de désignation, à savoir :

PROTÉGÉ : Lorsque l'information ne devrait être ni publiée ni communiquée à quelqu'un, sauf à des fins officielles

PROTÉGÉ (DÉLICAT) :
Comme l'information classifiée, l'information désignée n'a pas uniformément la même importance, mais elle doit, elle aussi, être protégée. La divulgation ou la perte de certains documents désignés pourrait en effet être particulièrement préjudiciable; il faut donc prendre des mesures de protection supplémentaires et marquer ces documents en conséquence, surtout lorsqu'ils sont expédiés à l'extérieur de l'unité qui les a préparés ou recueillis.

Les renseignements désignés doivent porter la cote de sécurité appropriée au moment où ils sont produits ou recueillis. Des indications particulières peuvent être utilisées pour expliquer la raison de la désignation. P. ex :

PROTÉGÉ – IMMIGRATION
PROTÉGÉ – CONSULAIRE
PROTÉGÉ – PERSONNEL (DÉLICAT)

Guide de classification de sécurité

Le *Guide de classification de sécurité* du Ministère (AECE 13 SUPP1 — Supplément nº 1 au *Manuel des instructions de sécurité*) vous permettra de savoir si vous devez classifier ou désigner des renseignements, comment le faire et qui consulter. On y trouve aussi les indications qui devraient accompagner les documents désignés.

Qui peut désigner ou classifier des renseignements?

Si les renseignements correspondent à un type déjà décrit dans le *Guide de classification de sécurité*, n'importe qui peut les classifier ou les désigner selon les instructions du Guide; si ce n'est pas le cas, seul un directeur adjoint ou quelqu'un occupant un poste plus élevé peut le faire.

Extraits de documents classifiés ou désignés

L'information provenant de matériel déjà classifié ou désigné est automatiquement classifiée ou désignée de la même manière que le document original. Par exemple, lorsque quelqu'un prépare une note documentaire concernant un document classifié SECRET, la note doit aussi être classifiée SECRET.

5. Protection des renseignements classifiés

Traitement des renseignements classifiés

Exigences minimales de conservation

Exigences minimales pour la conservation du matériel classifié qui se trouve dans une **zone protégée :**

TRÈS SECRET – armoire de sûreté approuvée munie d'une serrure à combinaison, classeur de sécurité muni d'une serrure à combinaison, ou coffre-fort.

SECRET – Classeurs de sécurité approuvés à 2 ou 4 tiroirs munis d'un double moraillon et d'un cadenas S & G à combinaison approuvé.

CONFIDENTIEL – Classeurs de sécurité approuvés à 2 ou 4 tiroirs munis d'un double moraillon et d'un cadenas S & G à combinaison approuvé.

PROTÉGÉ et PROTÉGÉ (DÉLICAT) – sur les étagères d'un coffre fort autorisé ou dans un contenant de sécurité approuvé.

REMARQUES : 1) On peut obtenir les armoires de sûreté en s'adressant à ISSG.

2) Les classeurs de sécurité approuvés à 2 ou 4 tiroirs peuvent être obtenus auprès de MFM. Toutefois, il ne faut pas les utiliser avant que ISSG n'ait apposé sa vignette de certification. Il faut également informer ISSG du déplacement ou de l'aliénation de ces classeurs.

Transmission de matériel classifié

On trouvera à l'annexe A à la fin du présent guide un tableau où sont résumées les exigences de sécurité pour la transmission de matériel classifié ou désigné.

Méthodes d'envoi

TRÈS SECRET

À l'intérieur de l'édifice de l'Administration centrale – L'information cotée TRÈS SECRET doit être placée dans deux enveloppes scellées marquées TRÈS SECRET et portant le numéro de dossier approprié ainsi que l'identité du récipiendaire et de l'expéditeur. L'enveloppe intérieure doit être scellée avec un ruban de sécurité. L'envoi doit être ensuite livré PAR PORTEUR à l'Unité des dossiers spéciaux MIRD (non pas la section ordinaire de livraison par porteur MIRM).

À l'extérieur du Ministère – La transmission de matériel TRÈS SECRET à d'autres ministères fédéraux de la Région de la capitale nationale doit être effectuée PAR PORTEUR par l'Unité des dossiers spéciaux (MIRD). Les documents doivent être placés dans deux enveloppes scellées clairement marquées TRÈS SECRET et PAR PORTEUR. L'enveloppe intérieure doit être scellée avec un ruban de sécurité. Les enveloppes doivent porter l'adresse complète du destinataire et le nom de la direction d'origine.

Les messagers qui livrent des documents TRÈS SECRET utilisent des contenants de sécurité approuvés (malette à documents) qui constituent « l'enveloppe extérieure » des envois TRÈS SECRET et SECRET.

> Pour obtenir des renseignements sur la transmission de matériel TRÈS SECRET **à l'extérieur** de la Région de la Capitale nationale, vous êtes invités à consulter le *Manuel des instructions de sécurité*.

SECRET, CONFIDENTIEL, PROTÉGÉ ET PROTÉGÉ (DÉLICAT)

À l'intérieur de l'édifice de l'Administration centrale – Le matériel SECRET, CONFIDENTIEL, PROTÉGÉ et PROTÉGÉ (DÉLICAT) doit être placé dans une enveloppe à ficelle (ou enveloppe ordinaire) scellée avec un autocollant de sécurité (Formulaire EXT 106). L'enveloppe doit porter le numéro de dossier ainsi que le nom du destinataire et de l'expéditeur. La livraison doit se faire PAR PORTEUR (MIRM) ou par un employé ayant une autorisation sécuritaire appropriée.

À l'extérieur du Ministère – Le matériel marqué PAR PORTEUR, SECRET, CONFIDENTIEL, PROTÉGÉ ou PROTÉGÉ (DÉLICAT) destiné à d'autres directions du Ministère et à d'autres ministères fédéraux de la Région de la capitale nationale est expédié par un messager ayant reçu une autorisation sécuritaire. Les documents doivent être placés dans une enveloppe scellée portant l'adresse du destinataire, la classification de sécurité et les mots PAR PORTEUR ainsi que le nom clairement indiqué de la direction d'origine. Dans ces cas, le contenant de sécurité autorisé (mallette à documents) est considéré comme l'équivalent d'une deuxième enveloppe « extérieure ». Le messager doit obtenir un reçu.

> Pour de plus amples renseignements sur la transmission de matériel SECRET ou CONFIDENTIEL **à l'extérieur** de la Région de la Capitale nationale, vous êtes priés de consulter les annexes du présent guide.

Matériel classifié à l'intention des missions à l'étranger

Le matériel classifié destiné à des missions à l'étranger doit être placé dans une enveloppe facilement identifiable sur laquelle doivent être clairement indiqués la cote de sécurité, le numéro assigné par la direction, et le nom de la direction ou de l'agent qui en fait l'expédition. Le matériel TRÈS SECRET doit être livré PAR PORTEUR à l'Unité des dossiers spéciaux (MIRD). Les autres documents classifiés et désignés doivent être livrés PAR PORTEUR à la salle principale du courrier (MIRM) au rez-de-chaussée de la Tour A.

> Pour de plus amples renseignements sur le recours aux services de courrier et de sacs à l'extérieur de la Région de la Capitale nationale et pour les missions à l'étranger, vous êtes priés de consulter le *Manuel des instructions de sécurité*.

Documents nécessitant un traitement spécial

Il arrive régulièrement que le Ministère doive préparer des documents qui, en raison de leur contenu, ont une signification spéciale autre que celle qui correspond à la classification de sécurité, par exemple des documents préparés à l'intention du Cabinet, ou des notes documen-

taires utilisées par les ministres aux réunions du Cabinet ou des comités du Cabinet. Avant de préparer ces documents, il faut consulter le *Manuel des instructions de sécurité* afin de prendre connaissance des renseignements concernant la classification, la préparation, la transmission, la conservation, le classement et la destruction du matériel classifié et désigné. Le *Manuel des instructions de sécurité* traite aussi de l'information classifiée de l'OTAN et les documents du Cabinet.

L'employé responsable d'un document doit garder le compte exact de **toutes** les copies faites, y compris les différentes ébauches. Un registre dans lequel seront notés la distribution, le retour ou la destruction de chaque copie du document doit être tenu. Chaque copie, y compris celle de chaque ébauche, doit être numérotée. Les copies devraient être remises sur signature d'un reçu seulement. Cette marche à suivre s'applique aussi à la préparation de cahiers d'information.

Matériel auxiliaire

Le matériel utilisé pour la préparation de documents de nature délicate doit être protégé de façon appropriée. Par exemple, les rubans de machine à écrire dont on s'est servi pour préparer le matériel classifié doivent être enlevés de la machine et rangés dans les armoires de sécurité en dehors des heures de travail et pendant toute période relativement longue où la machine n'est pas utilisée.

Élimination des rebuts classifiés

Il est essentiel de respecter à la lettre les pratiques établies en ce qui concerne l'élimination des rebuts contenant des renseignements classifiés. Les documents classifiés et désignés (sauf ceux qui sont marqués TRÈS SECRET) doivent être placés dans les contenants de sécurité métalliques qui se trouvent sur tous les étages de l'édifice. Ces contenants sont vidés régulièrement par des personnes ayant reçu une habilitation de sécurité, qui en détruiront le contenu selon les méthodes approuvées.

Les rebuts TRÈS SECRET seront détruits par déchiquetage, selon un procédé bien établi.

Il arrive parfois que des employés mettent du matériel classifié dans des contenants à rebuts sécuritaires et découvrent ensuite qu'ils

doivent le récupérer. Dans ce cas, il faut contacter le bureau du garde en chef (992-5452), qui enverra une personne habilitée de la Direction de la sécurité pour récupérer le document en question.

> Il est **strictement interdit** de mettre du matériel ou des documents classifiés destinés au rebut dans des contenants ordinaires, non fermés à clés ou non autorisés.

Garde des documents dans les bureaux

Les employés ont la responsabilité de voir à ce que l'information classifiée ou désignée qui se trouve dans leur bureau ou aire de travail soit toujours protégée.

Points à observer en matière de protection des documents :

- Sauf exceptions dictées par le bon sens, les portes et les fenêtres doivent être verrouillées et l'information classifiée ou désignée placée dans un classeur de sécurité fermé à clé lorsque l'employé s'absente de son bureau.

- Pendant les heures de travail, chaque employé est responsable de la sécurité dans son propre bureau et doit constamment veiller au respect des procédures de sécurité.

- Si, durant l'heure du déjeuner ou pendant une absence prolongée, il est impossible de laisser le bureau sous la supervision d'un membre du personnel ayant reçu une habilitation sécuritaire, toute l'information classifiée et désignée doit être mise sous clé dans des classeurs sécuritaires approuvés; le bureau doit ensuite être fermé de façon à empêcher l'entrée de personnes non autorisées.

- Les employés qui laissent leur bureau sous la supervision d'un membre du personnel ayant reçu une habilitation sécuritaire doivent s'assurer que l'information classifiée ou désignée est protégée adéquatement lorsque l'employé de garde part déjeuner, termine sa journée ou quitte lui-même le bureau.

- L'employé qui désire retourner à son bureau après les heures normales de travail ne doit pas laisser d'information classifiée ou désignée en vue dans son bureau pendant son absence, mais la mettre sous clé dans un classeur sécuritaire approuvé.

- En dehors des heures de travail, pendant les fins de semaine et les jours fériés, toute l'information classifiée ou désignée doit être rangée et tous les bureaux fermés de façon à empêcher l'entrée de personnes non autorisées.

Cartes d'absence

Afin d'empêcher que des documents classifiés ou désignés soient laissés sur le bureau de personnes absentes, des cartes d'absence (formulaire EXT 1431) obtenues de MFMG devraient être placées sur leur bureau.

6. Sécurité du COSICS et des systèmes informatisés

Politique sur la sécurité informatique

La politique sur la sécurité informatique du Ministère se trouve dans le *Manuel des instructions de sécurité.* Elle s'applique au fonctionnement ou à l'utilisation de tous les ordinateurs (mini-ordinateurs ou micro-ordinateurs) qui servent au traitement des données du Ministère; elle s'applique aussi aux travaux d'élaboration des systèmes et de programmation reliés à ces ordinateurs.

> Il faut tenir compte des exigences relatives à la sécurité dans l'élaboration des applications informatiques.

Politique sur la sécurité des micro-ordinateurs

> Les politiques du Ministère portant sur l'utilisation sécuritaire des micro-ordinateurs autonomes ou en réseaux se trouvent dans le *Manuel des instructions de sécurité.*

COSICS

Le Réseau canadien d'information et de communication protégées à accès direct (COSICS) doit être progressivement installé à l'Administration centrale, dans les missions et à d'autres endroits approuvés. Tous les employés doivent respecter les exigences de la politique sur la sécurité lorsqu'ils utilisent le COSICS ou qu'ils s'y relient. Les employés seront informés des critères de sécurité à mesure que le réseau sera établi.

Apposition de la cote de sécurité sur les documents

La politique sur la sécurité informatique exige que les rapports et les documents imprimés à partir du COSICS et d'autres systèmes informatisés portent visiblement la cote de sécurité sur la première page ou sur toutes les pages, selon que l'exige la cote de sécurité des données.

Inspections de la sécurité informatique

À l'Administration centrale, ISS applique un programme continu d'inspections de la sécurité informatique à divers points choisis ou au hasard. Ces inspections ont pour but de détecter les infractions à la sécurité.

Infractions

Les infractions à la sécurité informatique sont décelées au moyen d'inspections manuelles et de méthodes automatisées. Comme le veut le programme de dépistage des infractions de sécurité, les infractions répétées pourront entraîner une mise en garde de la part de la haute direction ou la révocation de l'habilitation de sécurité.

7. Sécurité du personnel

Politique

La politique du Ministère sur la sécurité du personnel se trouve dans le *Manuel des instructions de sécurité.* Elle s'applique aux fonctionnaires et aux employés contractuels du Ministère en poste au Canada et dans les missions, y compris le personnel recruté sur place à l'étranger.

Les questions se rapportant à la sécurité du personnel relèvent de ISSV.

Sauvegardes

Définition

Les sauvegardes concernant la sécurité du personnel sont établies au moyen d'un ensemble de vérifications portant sur les personnes qui traitent le matériel classifié ou désigné. Le filtrage du personnel se fait en fonction du type d'information ou de biens auxquels ils doivent avoir accès.

Filtrage du personnel

Le « besoin de savoir » est un des principes fondamentaux d'un bon programme de sécurité – l'accès aux renseignements est limité aux personnes qui en ont besoin pour exercer leurs fonctions. En outre, la politique du gouvernement sur la sécurité exige que les employés éventuels fassent l'objet d'une enquête comme condition de nomination à un nouveau poste. Ce processus s'applique aussi aux affectations et aux contrats. Le type de filtrage dépend du type de matériel que la personne doit utiliser.

> Personne ne peut avoir accès à du matériel désigné ou classifié tant que les vérifications appropriées n'ont pas été faites ou l'autorisation de sécurité obtenue.

Vérifications de la fiabilité

La vérification de base

La vérification de base de la fiabilité est obligatoire pour toute personne entrant à la fonction publique, et elle est une condition de la nomination. Le sous-secrétaire d'État aux Affaires extérieures peut en

dispenser les employés fédéraux déjà en fonction. Par ailleurs, elle n'est pas obligatoire pour les nominations, affectations ou contrats de moins de six mois. La vérification porte sur les points suivants :

- les données personnelles
- la scolarité et l'expérience professionnelle
- les accréditations et certifications
- les données sur l'emploi
- la fiabilité (auprès des employeurs précédents et des personnes citées comme référence)
- l'existence possible d'un dossier criminel (vérification préliminaire)
- la consultation du Système d'information sur les cessations d'emploi avec motif tenu par la Commission de la fonction publique. Il s'agit d'une liste des employés qui ont été mis à pied ou expulsés de la fonction publique avec motif

Vérification approfondie de la fiabilité

Une vérification approfondie de la fiabilité est requise lorsque la personne qui doit être embauchée, que ce soit par affectation, nomination ou contrat, devra avoir régulièrement accès à des renseignements désignés ou à des biens sensibles ou de valeur. Là aussi, la nomination est subordonnée à la vérification.

En plus des éléments compris dans la vérification de base, la vérification approfondie comprend les points suivants :

- une vérification des empreintes digitales
- une vérification du crédit
- d'autres vérifications si les fonctions du poste l'exigent

> La personne doit être informée de ce que comporte la vérification de fiabilité. Les renseignements personnels ne peuvent être utilisés pour la vérification approfondie sans le consentement de la personne qui en est l'objet.

Autorisations de sécurité

Les autorisations de sécurité sont nécessaires pour toute personne qui devra avoir accès à des informations ou des biens classifiés, peu importe

le type d'affectation, de nomination ou de contrat envisagé. Les enquêtes relatives aux autorisations de sécurité sont menées en plus des vérifications de base de la fiabilité. Les autorisations de sécurité sont essentiellement fondées sur des vérifications visant à établir la loyauté et la fiabilité de la personne en question; elles ne servent pas à vérifier la compétence professionnelle ou technique.

Il y a trois types d'autorisations de sécurité. Ils correspondent aux trois niveaux de classification :

Niveau 1 — accès à l'information cotée CONFIDENTIEL
Niveau 2 — accès à l'information cotée SECRET
Niveau 3 — accès à l'information cotée TRÈS SECRET

Le Service canadien du renseignement de sécurité mène les enquêtes de sécurité, à la demande de la Section de la sécurité du personnel (ISSV). Le sous-secrétaire d'État aux Affaires extérieures a délégué à cette dernière le pouvoir d'accorder les autorisations sécuritaires. Les renseignements personnels ne peuvent être utilisés pour l'autorisation de sécurité sans le consentement écrit de la personne faisant l'objet de l'enquête, et cette personne doit être informée des résultats. Les renseignements donnés sont protégés aux termes de la *Loi sur la protection des renseignements personnels.*

À moins d'avis contraire de la part de l'Agent de sécurité du Ministère (ISS), les employés des Affaires extérieures doivent, conformément à la politique ministérielle, détenir une autorisation de sécurité aux niveaux 2 ou 3 (SECRET ou TRÈS SECRET). Les employés permutants du service extérieur en poste à l'étranger doivent détenir une autorisation au niveau 3 (TRÈS SECRET). L'autorisation est valable pour une période allant jusqu'à dix ans. ISSV informe les employés lorsqu'elle est sur le point d'expirer.

Infractions à la sécurité et négligences

Définitions

Une **infraction** à la sécurité consiste en une divulgation non autorisée de renseignements classifiés ou désignés à des personnes qui n'ont pas droit de savoir. C'est le cas également lorsqu'il y a perte, vol ou endommagement délibéré d'équipement ou de matériel désigné ou classifié. Les infractions à la sécurité doivent être rapportées à l'Agent de sécurité du Ministère (ISS) dès qu'elles sont découvertes.

Les **négligences** sont des actions qui auraient pu mener à une infraction à la sécurité. Par exemple une personne commet une négligence lorsqu'elle :

- omet de classifier ou de désigner des renseignements selon la politique de la sécurité de l'information du Ministère
- classifie ou désigne des renseignements en contravention avec cette politique
- modifie, conserve, détruit ou retire sans autorisation des renseignements ou des biens classifiés ou désignés
- cause une interruption non autorisée de la communication de renseignements classifiés ou désignés
- néglige de mettre sous clé ou de protéger physiquement d'une autre manière l'information ou les biens classifiés ou désignés
- entre en communication avec le système COSICS ou d'autres ordinateurs du Ministère d'une façon interdite par la politique sur la sécurité informatique du Ministère

Sanctions

Le sous-secrétaire d'État aux Affaires extérieures peut, à sa discrétion, imposer des sanctions administratives ou disciplinaires, ou les deux, à ceux qui se rendent coupables d'infractions à la sécurité ou de négligences. Selon les circonstances et le dossier de l'employé, les sanctions peuvent consister en :

- une révocation du pouvoir de classifier
- la perte de l'autorisation sécuritaire et l'interdiction d'accéder au matériel classifié
- la perte du statut acquis par l'enquête de fiabilité approfondie et l'interdiction d'accéder au matériel sensible
- une réprimande verbale ou écrite, une suspension sans traitement, le congédiement
- l'annulation d'un contrat

Recours

L'employé à qui on refuse une autorisation sécuritaire ou pour lequel la vérification de fiabilité approfondie a donné des résultats négatifs peut en appeler de cette décision. Il en est de même lorsque des mesures disciplinaires sont imposées par le sous-secrétaire d'État aux Affaires extérieures.

Les recours contre les mesures disciplinaires, sauf contre la révocation de l'autorisation de sécurité, peuvent être invoqués conformément aux articles 90 et 91 de la *Loi sur les relations de travail dans la fonction publique.*

Les employés qui désirent en appeler d'une décision négative à la suite d'une enquête de base ou approfondie sur la fiabilité peuvent le faire en suivant les procédures normales de dépôt de griefs. Tous les griefs sur les vérifications de fiabilité doivent être adressées immédiatement au dernier palier.

C'est le Comité de surveillance des activités de renseignement de sécurité du gouvernement qui étudie les plaintes reçues à ce sujet. Toute personne à qui on a refusé une autorisation sécuritaire – employé, entrepreneur ou candidat de l'extérieur – peut demander qu'une telle étude soit menée.

Programme sur les infractions à la sécurité

Définition

Une infraction à la sécurité se définit comme une dérogation grave aux politiques sur la sécurité de l'information et sur la sécurité informatique qui pourrait compromettre le matériel classifié ou désigné, y compris les logiciels. Les infractions les plus courantes sont les classeurs et armoires de sécurité laissés ouverts après les heures normales de travail, les documents classifiés en vue sur les bureaux, les documents classifiés jetés dans les corbeilles à papier, les rubans de machine à écrire laissés dans les machines marquées « classifié », etc. Il y a aussi infraction à la sécurité lorsque l'on néglige de s'assurer que les visiteurs et les entrepreneurs (y compris les personnes qui font l'entretien de l'équipement) soient constamment escortés dans les zones réglementées.

Procédures

Des membres du Corps canadien des commissionnaires ayant une autorisation sécuritaire effectuent des rondes, généralement en dehors des heures de travail mais aussi parfois durant les heures normales de travail et les heures de pause, afin de s'assurer que le matériel classifié n'est pas susceptible d'être vu par des personnes non autorisées. Lorsqu'ils trouvent des classeurs ou des armoires de sécurité non fermés à clé ou des documents classifiés sur les bureaux, ils rédigent

un avis d'infraction à la sécurité et laissent l'original sur le bureau de l'intéressé. Le document classifié est saisi, placé dans une enveloppe scellée au moyen d'un autocollant portant la classification de sécurité appropriée, et livré en personne au Coordonnateur – aux infractions à la sécurité, pièce BG-239 (996-7191).

Le lendemain, il appartient à la personne qui a reçu l'avis d'infraction d'aller chercher le document confisqué auprès du Coordonnateur.

Un programme d'inspection de la sécurité informatique est constamment appliqué dans les bureaux du Ministère au Canada. Ce programme comprend des inspections manuelles par le personnel de la Direction de la sécurité et des membres du Corps canadien des commissionnaires ayant une autorisation sécuritaire, et des méthodes de dépistage automatique des infractions au COSICS et à d'autres systèmes informatisés du Ministère. La Section de la sécurité informatique (ISSC) et ISSG exercent une surveillance conjointe et évaluent les infractions.

ISSG prend très au sérieux les infractions à la sécurité. Toutes les dérogations sont rapportées au surveillant immédiat et au directeur de l'employé concerné et elles peuvent se solder par une mise en garde de la part de la haute direction ou par la révocation de l'autorisation sécuritaire.

ANNEXE A

Affaires extérieures et Commerce extérieur Canada — External Affairs and International Trade Canada

SÉCURITÉ DES DOCUMENTS À L'ÉDIFICE LESTER B. PEARSON — TABLEAU DE RÉFÉRENCE

Destination	1) PROTÉGÉ * 2) PROTÉGÉ « A »	1) CONFIDENTIEL 2) PROTÉGÉ (DÉLICAT) * 3) PROTÉGÉ « B » * 4) PROTÉGÉ « C »	SECRET
Dans l'édifice Lester B. Pearson	– adresser à la direction concernée dans une enveloppe à ficelle et sceller avec l'auto-collant EXT 106	– adresser à la direction concernée dans une enveloppe à ficelle et sceller avec l'auto-collant EXT 106	– addresser à la direction concernée dans une enveloppe à ficelle et sceller avec l'auto-collant EXT 106
Dans les missions diplomatiques, par l'entremise de MIRM	– adresser à **MIRM** dans une enveloppe à ficelle et sceller avec l'auto-collant EXT 106 **ou** – adresser dans une enveloppe spéciale EXT 2 ou EXT 3 avec la mention de la cote de sécurité et du numéro du document, et envoyer à MIRM	– adresser à **MIRM** dans une enveloppe à ficelle et sceller avec l'auto-collant EXT 106 **ou** – adresser dans une enveloppe spéciale EXT 2 ou EXT 3 avec la mention de la cote de sécurité et du numéro du document, sceller avec la bande approuvée et envoyer à MIRM	– adresser à **MIRM** dans une enveloppe à ficelle et sceller avec l'auto-collant EXT 106 **ou** – adresser dans une enveloppe spéciale EXT 2 ou EXT 3 avec la mention de la cote de sécurité et du numéro du document, sceller avec la bande approuvée et envoyer à MIRM
Dans la Région de la Capitale nationale	– une enveloppe gommée **sans cote** de sécurité – courrier de 1re classe	– une enveloppe gommée – cote de sécurité au coin supérieur droit de l'enveloppe – symbole de la direction et numéro du registre « **par porteur** » au coin inférieur gauche de l'enveloppe – sceller l'enveloppe avec la bande approuvée, et envoyer à MIRM	– une enveloppe gommée – joindre le bordereau EXT 34 au document – cote de sécurité au coin supérieur droit de l'enveloppe – symbole de la direction et numéro du registre « **par porteur** » au coin inférieur gauche de l'enveloppe – sceller l'enveloppe avec la bande approuvée, et envoyer à MIRM
Ailleurs au Canada	– une enveloppe gommée **sans cote** de sécurité – courrier de 1re classe	– préparer **deux** enveloppes gommées indiquant chacune l'adresse complète de l'expéditeur et du destinataire – indiquer la cote de sécurité au coin supérieur droit de l'enveloppe **intérieure** – sceller l'enveloppe intérieure avec la bande approuvée – inscrire la mention « **courrier de sécurité** » au coin supérieur droit de l'enveloppe **extérieure,** et envoyer à MIRM	– préparer **deux** enveloppes gommées indiquant chacune l'adresse complète de l'expéditeur et du destinataire – joindre le bordereau EXT 34 au document dans l'enveloppe **intérieure** – indiquer la cote de sécurité au coin supérieur droit de l'enveloppe intérieure – sceller l'enveloppe intérieure avec la bande approuvée – inscrire la mention « **courrier de sécurité** » au coin supérieur droit de l'enveloppe **extérieure,** et envoyer à MIRM

* Les catégories PROTÉGÉS « A », « B » et « C » ont été adoptées par certains autres ministères pour identifier le degré de sensibilité de l'information désignée « A » pour un document à faible sensibilité, « B » pour un document particulièrement sensible, et « C » pour un document extrêmement sensible. Toutefois, les cotes de sécurité PROTÉGÉ et PROTÉGÉ (DÉLICAT) **continueront d'être utilisées par AECEC** pour l'information désignée comme étant sensible, mais non d'intérêt national.

Note 1 – Il faudra inscrire, sur l'auto-collant EXT 106, **toutes les données nécessaires à l'acheminement** des documents lorsqu'il s'agit des catégories SECRET, CONFIDENTIEL, et PROTÉGÉ (DÉLICAT), ou lorsque le nom du destinataire est précédé de l'avertissement « RÉSERVÉ AU DESTINATAIRE SEULEMENT ». Ces données d'acheminement ne sont habituellement pas requises pour les autres catégories.

Note 2 – Pour les documents **TRÈS SECRET**, se reporter au Manuel des instructions de sécurité (MIS) et contacter la Section des dossiers spéciaux (MIRD).

EXT 1512 (05/90)

ANNEXE B

Affaires extérieures et Commerce extérieur Canada
External Affairs and International Trade Canada

SÉCURITÉ DES DOCUMENTS DANS LA RCN – TABLEAU DE RÉFÉRENCE

(Ailleurs qu'à l'Édifice Lester B. Pearson)

Destination	1) PROTÉGÉ * 2) PROTÉGÉ «A»	1) CONFIDENTIEL 2) PROTÉGÉ (DÉLICAT) * 3) PROTÉGÉ «B» * 4) PROTÉGÉ «C»	SECRET
À un emplacement satellite	– une enveloppe gommée portant l'auto-collant EXT 106	– une enveloppe gommée portant l'auto-collant EXT 106	– une enveloppe gommée portant l'auto-collant EXT 106
Dans la Région de la Capitale nationale, **y compris** l'Édifice Lester B. Pearson	– une enveloppe gommée **sans cote** de sécurité – courrier de 1re classe, ou levée par le préposé au courrier de MIRM	– une enveloppe gommée – cote de sécurité au coin supérieur droit de l'enveloppe – symbole de la direction et numéro du registre **«par porteur»** au coin inférieur gauche de l'enveloppe – sceller l'enveloppe avec la bande approuvée – levée par le préposé au courrier de MIRM	– une enveloppe gommée – joindre le bordereau EXT 34 au document – cote de sécurité au coin supérieur droit de l'enveloppe – symbole de la direction et numéro du registre **«par porteur»** au coin inférieur gauche de l'enveloppe – sceller l'enveloppe avec la bande approuvée – levée par le préposé au courrier de MIRM
Dans les missions diplomatiques, par l'entremise de MIRM	– adresser dans une enveloppe spéciale EXT 2 or EXT 3 avec la mention de la cote de sécurité et du numéro du document – levée par le préposé au courrier de MIRM	– adresser dans une enveloppe spéciale EXT 2 or EXT 3 avec la mention de la cote de sécurité et du numéro du document – sceller l'enveloppe avec la bande approuvée – levée par le préposé au courrier de MIRM	– adresser dans une enveloppe spéciale EXT 2 or EXT 3 avec la mention de la cote de sécurité et du numéro du document – sceller l'enveloppe avec la bande approuvée – levée par le préposé au courrier de MIRM
Ailleurs au Canada	– une enveloppe gommée **sans cote** de sécurité – courrier de 1re classe, ou levée par le préposé au courrier de MIRM	– préparer **deux** enveloppes gommées indiquant chacune l'adresse complète de l'expéditeur et du destinataire – indiquer la cote de sécurité au coin supérieur droit de l'enveloppe **intérieure** – sceller l'enveloppe intérieure avec la bande approuvée – inscrire la mention **«courrier de sécurité»** au coin supérieur droit de l'enveloppe **extérieure** – levée par le préposé au courrier de MIRM	– préparer **deux** enveloppes gommées indiquant chacune l'adresse complète de l'expéditeur et du destinataire – joindre le bordereau EXT 34 au document dans l'enveloppe **intérieure** – indiquer la cote de sécurité au coin supérieur droit de l'enveloppe intérieure – sceller l'enveloppe intérieure avec la bande approuvée – inscrire la mention **«courrier de sécurité»** au coin supérieur droit de l'enveloppe **extérieure** – levée par le préposé au courrier de MIRM

* Les catégories PROTÉGÉ «A», «B» et «C» ont été adoptées par certains autres ministères du gouvernement pour identifier le degré de sensibilité de l'information désignée «A» pour un document à faible sensibilité, «B» pour un document particulièrement sensible, et «C» pour un document extrêmement sensible. Toutefois, les cotes de sécurité PROTÉGÉ et PROTÉGÉ (DÉLICAT) **continueront d'être utilisées par AECEC** pour l'information désignée comme étant sensible, mais non d'intérêt national.

Note 1 – Il faudra inscrire sur l'auto-collant EXT 106 **toutes les données nécessaires à l'acheminement** des documents lorsqu'il s'agit des catégories SECRET, CONFIDENTIEL et PROTÉGÉ (DÉLICAT), ou que le nom du destinataire est précédé de l'avertissement «RÉSERVÉ AU DESTINATAIRE SEULEMENT». Ces données d'acheminement ne sont habituellement pas requises pour les autres catégories.

Note 2 – Pour les documents **TRÈS SECRET**, se reporter au Manuel des instructions de sécurité (MIS) et contacter la Section des dossiers spéciaux (MIRD)

EXT 1512-1 (05/90)

NOTES

HEADQUARTERS SECURITY HANDBOOK

...An Employees' Guide

External Affairs and International Trade Canada

Canada

LESTER B. PEARSON BUILDING
EMERGENCY TELEPHONE NUMBERS

There are **RED EMERGENCY TELEPHONES** located outside stairwells on each floor in each tower of the building. These are connected directly to ISSG Building Emergency Central Control. Employees are requested to use them immediately in the event of a fire or any other type of emergency. If unable to reach the red telephone, dial **992-1150** for the Building Emergency Control Centre.

Following is a list of emergency telephone numbers.

Building Emergency Control Centre	992-1150
Ottawa Police Emergency	8-911
Ottawa Fire Department	8-911
Ambulance Emergency	8-911
Health Unit	996-9227
Main Lobby Reception Desk	995-5859
Security Division (ISSG)	992-5452

External Affairs and International Trade Canada
Affaires extérieures et Commerce extérieur Canada

Contents

1. Introduction

This handbook is published by the Departmental Security Officer (ISS).

The handbook summarizes and explains the main provisions of the Departmental Security Policies which are applicable at Headquarters. It contains only highlights and should not be read as a substitute for the policies. For further information, consult the *Manual of Security Instructions* or the appropriate ISS Section which in most cases will be ISSG.

Certain aspects of the Physical Security provisions and the Emergency Procedures provisions apply specifically to the Lester B. Pearson Building. Departmental employees and contractor staff working in other buildings in Ottawa or at locations elsewhere in Canada, including conference sites, must adhere to the specific security and emergency arrangements which prevail.

2. Physical Security

Security zones and areas

The departmental security system divides the Lester B. Pearson Building into a number of security zones for the purposes of controlling access and to protect all government assets against loss, damage, theft and compromise.

Public area

The main floor of the building is open to the public. In this public area is located the departmental library, cafeteria and the Royal Bank of Canada. Also included in the public area are the auditorium, main conference room and lobby area.

Sensitive area

All four towers are designated as Sensitive Areas and access to these towers is controlled by members of the Canadian Corps of Commissionaires. Access to the Sensitive Areas is restricted to persons with the appropriate building passes or to **escorted visitors.**

Security zone

Within the Sensitive Areas there are Security Zones which have restricted access to authorized persons only. Access to some, but not all, Security Zones is further controlled by the use of combination-lock doors and barriers.

Restricted access signs

Within the Sensitive Areas, prominently displayed signs such as "Security Zone" are used to indicate these highly secure and/or sensitive areas. Additional signs "Authorized Personnel Only" may be used. Only persons on work-related business are allowed to enter these areas.

Reception area (Tower A)

Floor 9 of Tower A is a reception area where departmental functions are hosted for visitors. Visitors must be appropriately escorted to and from the floor through the Tower A Sensitive Area; they must not be allowed unescorted access to other floors of Tower A.

Access and egress control

Building passes

Building passes are issued by ISSG for the purpose of controlling access to the four towers of the Lester B. Pearson building. Employees of the Department and other designated personnel are issued the passcard only after their security clearance is approved by ISSV. The passcard must be returned to ISSG upon transfer or termination of employment. The loss of a passcard should be reported at once to the Security Operations Officer.

Access during silent hours

Employees must be in possession of a valid departmental building pass and sign the access and egress register in order to be granted access to departmental accommodation after normal working hours, i.e. after 18:00 hours on working days, all day Saturday, Sunday and holidays.

Parking permits

Parking permits are issued by MFM and any questions concerning the issue of these permits should be directed to that division. ISSG, through a special arrangement with the RCMP, enforces the parking regulations established by the *Government Property Traffic Act.*

Canadian Corps of Commissionaires

The Corps of Commissionaires controls the access to the building and provides an escort service for all non-departmental persons who visit departmental employees. Visitors are escorted to the employee they wish to see and it is that employee's responsibility to escort the visitor(s) back to the main lobby when the visitor's business is concluded.

Visitors – employee responsibilities

Individuals who do not have passes must be escorted at all times while they are in the Sensitive Areas and Security Zones of the Lester B. Pearson Building. Visitors and equipment service personnel who have appointments with departmental employees are escorted by the ISS Visitors Escort Service or by an employee to the employee's office or place of work. During the course of and when business or work is finished, the visitor **must** be escorted until back in the main lobby. This security measure is required

to ensure that visiting individuals are not able to move unescorted throughout the building, including areas where sensitive items are being handled and/or discussed.

Violation of this responsibility is a security infraction.

Silent hours – employee responsibilities

Employees frequently remain in the office after normal Ottawa business hours. Although the building is patrolled by the ISS Security staff during silent hours, it is required by the Canada Labour Code, in the interest of employee safety in the event of emergencies, that Security staff are aware of employees who are in the building.

Employees remaining in the building and working alone during silent hours must advise the Front Desk Security Officer (main lobby) at 995-5859.

Locks and combinations

S & G combination padlocks

All employees are responsible for the safeguarding of all classified material in their possession. Approved S & G combination padlocks may be obtained by telephoning 992-6679 (ISSG) for delivery.

Changing combinations

The combination setting of a dial lock shall be given the same protection as the highest classified matter it protects. The combination settings should be changed: every six months; when any person knowing the combination is transferred, released or no longer require access to the security container; and when the combination setting has been or may have been compromised.

Keys to offices

Keys to offices must be protected and not copied; spare keys should be controlled by Divisional secretaries. New keys and/or locks may be obtained by telephoning 992-6679 (ISSG) for service.

Failure to adequately safeguard keys is a security infraction.

Protection of personal and Government property

Procedures

It is the employees' responsibility to protect their personal property. Purses, wallets and money should be kept in their possession or secured at all times and items of sentimental value should be locked away during silent hours.

It is also the employees' responsibility to safeguard attractive Government property such as calculators, computer equipment, tape recorders, cameras, etc., in locked cabinets or rooms when not in continued use.

Report all losses and thefts

All losses or thefts must be reported immediately to Security Division, 996-4731 (ISSG). Prompt reporting of such incidents will assist Security Officers in their investigations.

3. Emergency Procedures

Requirements

Part XVII of the *Canada Occupational Safety and Health Regulations*, (issued under the *Canada Labour Code*) states the requirement for organizing a Building Fire Emergency Organization (B.F.E.O.) in all Government of Canada occupied buildings. The Organization is operational during normal working hours. Each floor is served by volunteer employees who, in addition to their regular duties, conduct checks for safety or fire hazards.

Responsibilities

ISSG is responsible for developing and implementing all procedures, orders and instructions relating to fires and other emergencies affecting the safety of personnel. In addition, it ensures the training of all employees and supervises the evacuation procedures during any emergencies.

Training

B.F.E.O. members are trained in the following:

- First Aid
- Fire/Emergency Procedures
- Use of Fire Extinguishers
- Emergency Threat Procedures
- Evacuation Procedures

Building emergency procedures

Emergency procedures have been developed for the Lester B. Pearson Building and are available in all Divisions. These procedures have been approved by the Director Security Division and the Chairpersons of the Pearson Building Occupational Safety and Health Committee.

These procedures are designed to provide a prompt and effective response to a wide variety of possible operational emergency events in the Lester B. Pearson Building. These can include a fire alert, a medical or security emergency, or a significant building equipment failure, which will require a response from building emergency services or municipal emergency services.

Experience shows that most people will react to an emergency situation in a sensible manner although each might respond in quite different ways. A simple set of emergency procedures, understood and practiced by both the emergency organization and the occupants, has the best prospect of providing the most coordinated and effective response to an emergency. Building occupants are encouraged to take the time to read and consider these procedures so that the collective response to an emergency will be the safest possible for all concerned.

The Building Emergency Procedures should not be mistaken for the departmental Emergency Preparedness/Crisis Management plans and procedures. The latter may become directly involved in building emergencies under certain circumstances, e.g., if a building-related problem could seriously harm the operations of the department, or if a damaging incident such as a fire requires that a "recovery" plan be instituted, or if the incident is Regional, National, or International in nature.

The following are the priorities of the Building Emergency Procedures.

1. Personal safety for all occupants of the Lester B. Pearson Building;

2. Protection and preservation of all information, systems and operations considered critical for the fulfilment of the departmental mandate; and

3. Safeguarding of all other private and departmental operations and assets.

Pearson building emergency control centre

This is the first number to call for most emergency situations which might involve

Fire – Evacuation
Medical Emergency – Ambulance, Health Unit, First Aid
Bomb Threat – Telephone, Parcel
Police & Security – Crimes, Disturbance, Intrusion
Building Systems – Equipment, Utilities
Disaster Events – Warning, Response, Organizations

Use the "Red Emergency Telephones", telephone 992-1150, or use the Fire Alarm Pull Station as appropriate.

The Control Centre is located in the basement of Tower B. It is a 24 hour operation centre which has a bilingual staff of Canadian Corps of Commissionaires who are thoroughly trained and familiar with every aspect of the building. They have radio communications to areas of the building during regular work hours and to selected areas in silent hours. The centre monitors all of the security and fire alarms in the building and the Red Emergency Telephone system. The voice communication system is managed from this point with well over 100 phones installed throughout the building. A complete set of floor plans and keys is maintained to serve the needs of the Ottawa Fire Department when they respond to an emergency.

Upon receiving notification of an emergency the Emergency Control Centre will communicate with all emergency response services:

- Municipal and Regional Emergency Response Services;
- Other External Emergency Services;
- Pearson Building Emergency Services; and
- Building Emergency Organization.

Floor emergency officers

A Chief Floor Emergency Officer is appointed for each floor of each Tower.

A Floor Emergency Officer is appointed for each work area on a floor.

Mobility-impaired employees

Those who have a mobility or sensory impairment, as well as those who may be temporarily impaired because of an injury or medical problem, are asked to make themselves known to the person or persons who agree to be their personal monitor, the Floor Emergency Officer in their area, and the Emergency Control Centre. In an emergency the building's Emergency Control Centre and the Ottawa Fire Department can use this information to manage the situation safely. If, on the other hand, the person with the condition does not wish to disclose his/her condition, the individual concerned should at least inform the Floor Emergency Officer as soon as an alert is sounded.

4. Information Classification for Security Purposes

What needs to be safeguarded?

At a minimum, information and assets that the department possesses should receive the reasonable care consistent with basic good administrative practice.

Beyond this, some information and assets are more sensitive or valuable and therefore require more stringent safeguards. In line with the provisions of the *Access to Information Act,* the *Privacy Act,* and the Government Security Policy, the department has grouped its information holdings into three categories:

- material that relates to the national interest
- material that lies outside the national interest but is nonetheless sensitive or valuable
- all other material, not all of which is in the public domain

If information can reasonably be expected to qualify for an exemption under the *Access to Information Act* or the *Privacy Act,* it must be either classified or designated.

Material assets important to the national interest or other sensitive or valuable assets also require more than basic protection. This includes, for example, all COSICS computer equipment.

Information given in confidence by other governments must be treated according to any agreements or understandings negotiated with them.

Information classified in the national interest

The Government Security Policy stipulates that information must be classified if its unauthorized disclosure or compromise could reasonably be expected to injure the national interest. For the purposes of the Security Policy, the "national interest" involves the "social, economic and political stability of Canada and, thereby, the security of the nation". Generally, the kind of information that is considered sensitive in the national interest is described in the access and privacy exemptions as involving:

- federal-provincial relations, international affairs, defence or the economic interests of Canada

- advice and recommendations connected with the above information
- information involving security and intelligence or the security clearance process.

> Under no circumstances may information be classified in order to conceal violations of law, inefficiency or administrative error, to avoid embarassment or to restrain competition.

Information designated as PROTECTED (SENSITIVE)

Certain information cannot be disclosed under the access and privacy legislation because of the injury disclosure could cause to particular public or private interests. This information must be designated as PROTECTED (SENSITIVE) if it could reasonably be expected to qualify for an exemption under the access and privacy legislation because it involves:

- law enforcement investigations
- the safety of an individual
- the government's competitive position
- research, testing procedures and audits
- the business information of a third party
- solicitor-client privilege
- other levels of government (and was given in confidence)
- medical records
- individual members of the public or federal employees
- matters that other laws, like the *Statistics Act,* prohibit disclosing

Information designated as PROTECTED – PERSONAL

The Government Security Policy makes a special point that all personal information must be given enhanced protection.

Certain information about departmental employees is sensitive and must receive enhanced protection, such as

- salaries (other than salary ranges)
- appraisals
- medical records
- conflict of interest declarations

Advice connected with information designated as sensitive must also be assessed for the potential injury it can cause. It, too, may be designated.

> Bear in mind that it is most important to protect any advice given in making decisions that directly affect individuals.

Material assets

Certain equipment or material is essential for the security of classified information. Advice on identifying and safeguarding it is available from ISSG. All COSICS equipment and many typewriters, word processors and microcomputers are in this category of equipment.

Negotiable assets, valuable equipment, or equipment critical to a departmental operation are to be designated as valuable or sensitive. Guidance on designating assets and how they should be protected is available from ISSG.

Classification and designation

Levels of classification and designation

There are three levels of classification, as follows:

TOP SECRET:	When compromise might reasonably cause exceptionally grave injury to the national interest. In this regard, compromise means any of disclosure, destruction, removal, modification or interruption. The impact must be great, immediate and irreparable. Obviously, the amount of information that merits this classification level is very limited.
SECRET:	When compromise might reasonably cause serious injury to the national interest.
CONFIDENTIAL:	When compromise might reasonably cause injury to the national interest. Most of the information or assets meriting classification clearly falls in this category.

The Canadian Government does not use the classification RESTRICTED. The term is used, however, for RESTRICTED NATO or OECD (Organization for Economic Cooperation and Development) information and must be treated as PROTECTED.

Classified information must be marked with its appropriate level at the time it is created or collected.

There are two levels of designation, as follows:

PROTECTED: When the information contained therein should not be published or communicated to any person, except for official purposes.

PROTECTED (SENSITIVE): Like Classified information, Designated information varies in its sensitivity. It must all be safeguarded. However, some of this Designated information could cause particular harm if it is disclosed or lost; it therefore warrants additional safeguards and should be marked to signal that fact, especially when it is sent outside the unit that created or collected it.

Designated information must be marked with its appropriate level at the time it is created or collected. Explanatory caveats may be used to further explain the reason for designation e.g.

PROTECTED – IMMIGRATION
PROTECTED – CONSULAR
PROTECTED – PERSONAL (SENSITIVE)

Departmental Security Classification Guide

The Departmental *Security Classification Guide* (Supplement No. 1 of the *Manual of Security Instructions*) will tell you whether to classify or designate information, how to do it and whom to consult. It also gives the caveats which should be used for designated information.

Who can designate or classify information?

If the information is of a type already identified in the *Security Classification Guide* anyone may classify or designate it according to the Guide's instructions. If the information is not mentioned in the guide, it can be classified or designated only by a Deputy Director or above.

Extracts from classified or designated material

Information derived from material that is already classified or designated is automatically classified or designated to match the original information. For instance, if a document is classified as SECRET, a person preparing a briefing note on it simply classifies the briefing material as SECRET.

5. Protection of Classified Information

Handling of classified information

Minimum storage requirements

The absolute minimum storage requirements for classified material in a **guarded area** are:

TOP SECRET – approved security shell (locker safe) with dial combination, a secure file with dial combination, or a vault.

SECRET – approved security file cabinet with double hasp and approved S & G combination padlock.

CONFIDENTIAL – approved security file cabinet with double hasp and approved S & G combination padlock.

PROTECTED and PROTECTED (SENSITIVE) – open shelving in an approved vaulted area or in an approved security container.

NOTES:

(1) Security shells (locker safes) are obtained from ISSG.

(2) Approved 2 or 4 drawer security file cabinets are obtained from MFM. However, they must not be used unless they bear the ISSG Certification Sticker. ISSG must also be notified of any relocation or disposal of such cabinets.

Transmission of classified material

A chart summarizing the security requirements for the transmission of classified and designated materials can be found in Annex A at the end of this handbook.

Mailing procedures

TOP SECRET

Within Headquarters Building – TOP SECRET information must be placed in double sealed envelopes marked TOP SECRET and bearing the appropriate file number and designations of addressee and sender. The inner envelope must also be sealed with security tape. This must be delivered BY HAND to the Special Records Unit MIRD (not to the regular outgoing BY HAND section MIRM).

Outside the Department – TOP SECRET material for transmission to other Government Departments in the National Capital Region must be handled by the Special Records unit (MIRD) for BY HAND delivery. Such documents are to be placed in double sealed envelopes, clearly marked TOP SECRET and BY HAND. The inner envelope must also be sealed with security tape. The envelopes must bear the complete address of the addressee and the name of the sending Division.

Messengers delivering TOP SECRET material use approved locked security containers (attaché case) which constitutes the "outer cover" of TOP SECRET and SECRET packages.

> Attention is invited to the *Manual of Security Instructions* for information regarding the transmission of TOP SECRET material **outside** the National Capital Region.

SECRET, CONFIDENTIAL, PROTECTED AND PROTECTED (SENSITIVE)

Within Headquarters Building – SECRET, CONFIDENTIAL, PROTECTED and PROTECTED (SENSITIVE) material must be placed in a string envelope (or sealed envelope) which must be sealed with a security classification sticker (Form EXT 106) which should bear the file number and names (or acronym) of the addressee and sender. Delivery must be BY HAND (MIRM) and/or appropriately security-cleared employee.

Outside the Department – BY HAND. — SECRET, CONFIDENTIAL, PROTECTED and PROTECTED (SENSITIVE) material for other EAITC Divisions and Government Departments in the National Capital Region is sent by security-cleared messenger. It must be contained in a single sealed envelope bearing the address of the addressee, the security

classification and the words BY HAND and the name of the originating Division clearly marked. In such cases the approved security container (attaché case) is considered the equivalent of a second or "outer" envelope. A receipt must be obtained by the messenger.

> You may also refer to Annex A to this handbook regarding the transmission of SECRET, CONFIDENTIAL and PROTECTED material outside the National Capital Region.

Classified material for missions abroad

Classified material destined for transmission to missions abroad is to be enclosed in a distinctive envelope which must clearly indicate the security classification, the divisional number of the documents and the name of the originating Division or officer. TOP SECRET material must be delived BY HAND to the Special Records Unit (MIRD). Other classified and designated material must be delivered BY HAND to the Main Mail Room (MIRM), Ground Floor, Tower A.

> Attention is invited to the *Manual of Security Instructions,* which details instructions for the use of Mail and Bag Service outside the National Capital Region and for Missions Abroad.

Documents requiring special handling

The Department is regularly required to prepare documents which, because of their content, have special significance in addition to that indicated by the level of security classification e.g., documents prepared for the consideration of Cabinet, or Briefings used by Ministers in Cabinet or Cabinet Committee. Prior to the preparation of such documents the *Manual of Security Instructions* should be reviewed for information dealing with the classification, preparation, transmission, custody, storage and destruction of classified and designated material. The *Manual of Security Instructions* also deals with NATO Classified Information and Cabinet Documents.

The responsible employee must ensure that a strict accounting is maintained at all times for **all** copies of a document, including successive drafts. A log is to be maintained for the distribution and return or destruction of each copy of the document. Each copy, including copies of each draft, is to be numbered. Copies should only be issued against a signed receipt. Similar practices are to be followed when preparing Briefing Books.

Auxiliary materials

Materials used in the preparation of sensitive documents must be appropriately protected. For instance, typewriter ribbons used on machines which process classified material must be removed from the typewriter and stored in a security cabinet during silent hours and other extended periods when the machine is unattended.

Disposal of classified waste

It is imperative that waste material containing classified information be disposed of in a rigidly enforced manner. Classified and designated documents up to and including SECRET must be placed in metal security containers which are located on all floors of the building. These containers are regularly emptied by security-cleared personnel, for destruction in accordance with approved procedures.

TOP SECRET waste is disposed of by shredding in a rigidly prescribed manner.

Occasionally, employees place classified material in approved security waste containers which they later find needs to be retrieved. When this occurs, the Security Desk (992-5452) should be contacted to despatch a security-cleared person from Security Division to retrieve the required documents.

> Under **no circumstances** is it permissible to place classified waste materials and documents in a regular, unlocked or unapproved waste containers.

Document custody in offices

Employees are responsible for ensuring that all classified or designated information in their office or work place is protected at all times.

Protection should be given in the following manners:

- Subject to common sense exceptions, during absence from the office, doors and windows must be securely locked and classified or designated information must be returned to a security container, which is to be locked.

- During working hours, every employee is responsible for the security of his or her own office and must ensure that office security procedures are observed at all times.

- If, during lunch hours or any lengthy absence during working hours, it is not possible to leave an office under the effective supervision of a security-cleared member of the staff, all classified and designated information should be put away and locked in approved security containers; the office should then be secured as usual against unauthorized entry.

- Employees who leave their offices under the effective supervision of a security cleared member of the staff must ensure that any classified or designated information is adequately protected if the "custodian" employee leaves for lunch, at the end of that persons working hours, or leaves the office for any period of time.

- An employee who wishes to return to her or his office to work after normal working hours should not leave classified or designated information exposed in that office while it is unattended. Classified or designated information should be locked away in an approved security container until the occupant returns.

- During silent hours, week-ends and holidays, all classified and designated information must be put away and all offices must be locked and secured against unauthorized entry.

Absent card

In order to prevent classified and/or designated documents and/or materials being delivered and left on desks in the absence of employees, absent cards (form EXT 1431) are available from MFMG and should be placed on desk tops for the duration of an employee's absence.

6. COSICS and EDP Security

EDP Security Policy

The Departmental EDP Security Policy is contained in the *Manual of Security Instructions*. The policy applies to the operation or use of all computers, both minicomputers, and microcomputers which process departmental data or information; it also applies to the system development and programming activities related to these computers.

> Security requirements must be included in the design of computer-based applications.

Microcomputer security policy

> Departmental policies covering the secure use of micro-computers, both standalone and networked, are contained in the *Manual of Security instructions*.

COSICS

The Canadian On-line Secure Information Communication System (COSICS) is scheduled to be progressively installed at Headquarters, Missions and other approved locations. All employees must adhere to security policy requirements when using or interfacing with COSICS. As COSICS is established, departmental employees will be briefed on its security requirements.

Security classification on documents

The EDP Security Policy requires that reports and documents printed by COSICS and other EDP Systems contain the security classification prominently displayed on the first or on all pages, as required by the security classification of the data.

EDP security inspections

A continuous program of EDP Security Inspections is undertaken by ISS at Headquarters, on both a selected basis and at random. These are aimed at detecting breaches and violations of security.

Infractions

EDP Security Infractions are detected by manual inspections and automated infraction detection methods. As part of the Security Infraction Program, repeated violations may result in counselling by senior management or revoking of security clearance.

7. Personnel Security

Policy

The Departmental Personnel Security Policy is contained in the *Manual of Security Instructions.* The policy applies to departmental employees and contract staff in Canada and at Missions, including locally-engaged staff at Missions.

Matters related to Personnel Security are dealt with by ISSV.

Safeguards

Definition

Personnel Security safeguards are the set of controls on the people that handle Classified or Designated material. The screening of personnel is linked to the kind of information or assets they will deal with.

Screening personnel

A basic tenet of good security is the "need to know" principle – limiting access to material to those people who must have access to it to do their job. In addition, the Government Security Policy requires that prospective employees pass a screening process as a condition of appointment to any new position. The screening process also applies to assignments and contracts. The type of screening depends on the type of material they must handle.

> Until the appropriate checks or clearances on an individual are complete, that person cannot have access to Designated or Classified material.

Reliability checks

The Basic Reliability Check

The Basic Reliability Check is mandatory for all new appointees to the Public Service, and is a condition of their appointment. The Under-

Secretary of State for External Affairs may waive it for current federal employees and it is not mandatory for appointments, assignments or contracts of less than six months. The Basic Reliability Check entails:

- verifying personal data
- verifying educational and professional qualifications
- accreditations or certifications
- checking employment data
- checking reliability with previous employers and references
- a name check of criminal records
- a check of the Separation for Cause Information System maintained by the Public Service Commission. This is a listing of employees who have been released or rejected on probation or dismissed or discharged from the Public Service for cause.

The Enhanced Reliability Check

An Enhanced Reliability Check is required when the person to be hired, whether by assignment, appointment or contract, will have consistent and regular access to Designated information or to sensitive or valuable assets. Again, this check is a condition of appointment.

In addition to the elements of the Basic Reliability Check, the Enhanced Reliability Check may require:

- a fingerprint check
- a credit check
- other checks, if the duties of the job so indicate.

> The person must be told what the reliability check will involve. Personal information cannot be used for this enhanced reliability check without the consent of the person to be checked.

Security clearances

Security clearances are required for anyone who will need access to Classified information or assets, regardless of the type of assignment, appointment or contract involved. Security clearances are carried out in addition to a basic reliability check. In essence, clearances are based on checks to establish loyalty and reliability; they do not verify professional or technical competence.

There are three levels of security clearance. They parallel the three levels of clasification:

Level 1 – access to CONFIDENTIAL
Level 2 – access to SECRET
Level 3 – access to TOP SECRET

The Canadian Security Intelligence Service carries out security screening investigations at the request of the Personnel Security Section (ISSV). The latter have delegated authority from the Under-Secretary of State for External Affairs to grant clearances. Personal information cannot be used for a security clearance without the signed consent of the person to be screened, and the individual must be advised of the findings. The information provided is protected under the *Privacy Act.*

It is departmental policy that departmental employees in Canada be cleared to levels 2 or 3 (SECRET or TOP SECRET), unless otherwise authorized by the Departmental Security Officer (ISS). Members of the rotational foreign service posted abroad require a level 3 (TOP SECRET) security clearance. Security clearances are valid for a period of up to ten years. ISSV will notify employees when existing security clearances are due to expire.

Breaches and violations of security

Definitions

A **security breach** is the unauthorized disclosure of Classified or Designated information to those who have no right to it, or the loss, theft or deliberate damage of Designated or Classified equipment or material. Security breaches must be reported immediately on detection to the Departmental Security Officer, ISS.

Security violations are events that could have led to a security breach, but did not. A security violation occurs, for instance, when a person:

- fails to classify or designate information according to the departmental Security of Information Policy
- classifies or designates information in contravention of the departmental Security of Information Policy

- alters, keeps, destroys or removes Classified or Designated information or assets without authorization
- causes an unauthorized interruption in the communication of Classified or Designated information
- fails to lock up or otherwise physically protect Classified or Designated information or assets
- accesses or operates COSICS and/or other departmental computers in violation of the departmental EDP Security Policy

Sanctions

The Under-Secretary of State for External Affairs has the discretion to apply administrative or disciplinary sanctions, or both, for security breaches or violations. The possible sanctions, depending on the circumstances and the past record of the employee, are:

- revocation of classification authority
- removal of security clearance and loss of access to classified material
- removal of enhanced reliability status and loss of access to sensitive material
- verbal or written reprimand, suspension without pay, dismissal
- cancellation of contract.

Redress

Redress is available when a security clearance or enhanced reliability status has been denied. It is also available for any disciplinary action taken by the Under-Secretary of State for External Affairs.

Redress from disciplinary sanctions, except the removal of security clearances, can be sought through Sections 90 and 91 of the *Public Service Staff Relations Act.*

Employees who wish to challenge a decision about a basic or enhanced reliability check may do so through normal grievance procedures. All grievances concerning reliability checks must go immediately to the final level.

The Security Intelligence Review Committee of the Government investigates complaints about the denial of security clearances. A review is available to anyone who is denied a security clearance, including employees, contractors and outside candidates.

Security infractions program

Definition

A Security Infraction is defined as a serious non-observance of the Security of Information Policy or the EDP Security Policy which could result in the compromise of classified or designated material, including computer software. The most common causes with respect to security of information are security cabinets and security shells left open after normal working hours, classified documents left out on desk tops, classified documents found in waste containers in offices, typewriter ribbons left in machines labelled "classified", etc. Failing to ensure that visitors and contractors (including equipment service personnel) are escorted at all times in controlled areas is also deemed to be a security infraction.

Procedures

Security patrols are conducted by security-cleared members of the Canadian Corps of Commissionaires, generally during silent-hours but possibly during normal working and break periods, to ensure that classified material is not exposed to unauthorized persons. When unlocked cabinets or security shells, or exposed classified documents are found in offices, a Security Infraction Notice is written and the original copy is left on the individual's desk. The classified document is confiscated, placed in an envelope which is sealed with a sticker bearing the appropriate security classification, and hand-delivered to the Security Infractions Coordinator, Room BG-239 (996-7191).

It is the responsibility of the individual who receives the Security Infraction Notice, to pick up the confiscated documents and materials from the Coordinator the following working day.

An EDP Security inspection program is continually applied on departmental premises in Canada. This involves manual inspection by personnel of the Security Division and security-cleared members of the Canadian Corps of Commissionaires, and, automated infraction detection methods in COSICS and other departmental computer systems. The EDP Security Section (ISSC) and ISSG jointly monitor and assess EDP security infractions.

Security Infractions are taken very seriously and are monitored by ISSG. All violations are reported to the employee's immediate supervisor and Director and may result in counselling by senior management or revocation of security clearance.

ANNEX A

External Affairs and International Trade Canada | Affaires extérieures et Commerce extérieur Canada

DOCUMENT SECURITY IN THE LESTER B. PEARSON BUILDING — REFERENCE CHART

Destination	1) PROTECTED * 2) PROTECTED "A"	1) CONFIDENTIAL 2) PROTECTED (SENSITIVE) * 3) PROTECTED "B" * 4) PROTECTED "C"	SECRET
Within Lester B. Pearson Building	– address string-tie envelope to Divison and close with sticker EXT 106	– address string-tie envelope to Division and close with sticker EXT 106	– address string-tie envelope to Divison and close with sticker EXT 106
Diplomatic Missions via MIRM	– address string-tie envelope to **MIRM** and close with sticker EXT 106 **or** – enclose in special envelope EXT 2 or EXT 3 annotated with security marking and document number; and send to MIRM	– address string-tie envelope to **MIRM** and close with sticker EXT 106 **or** – enclose in special envelope EXT 2 or EXT 3 annotated with security marking and document number; close with approved tape and send to MIRM	– address string-tie envelope to **MIRM** and close with sticker EXT 106 **or** – enclose in special envelope EXT 2 or EXT 3 annotated with security marking and document number; close with approved tape and send to MIRM
Within National Capital Region	– one gum-sealed envelope **without** security marking – first class mail	– one gum-sealed envelope – security marking on upper right-hand corner of envelope – Divisional symbol and "**by-hand**" number on lower left-hand corner of envelope – close envelope with approved tape, and send to MIRM	– one gum-sealed envelope – enclose receipt form EXT 34 with document – security marking on upper right-hand corner of envelope – Divisional symbol and "**by-hand**" number on lower left-hand corner of envelope – close envelope with approved tape, and send to MIRM
Elsewhere in Canada	– one gum-sealed envelope **without** security marking – first class mail	– prepare **two** gum-sealed envelopes, each with complete address of sender and receiver – security marking on upper right-hand corner of **inner** envelope – close inner envelope with approved tape – print "**Security Mail**" on upper right-hand corner of **outer** envelope and send to MIRM	– prepare **two** gum-sealed envelopes, each with complete address of sender and receiver – enclose receipt form EXT 34 with document in **inner** envelope – security marking on upper right-hand corner of inner envelope – close inner envelope with approved tape – print "**Security Mail**" on upper right-hand corner of **outer** envelope and send to MIRM

* The categories of PROTECTED "A", "B", and "C" have been adopted by some other government departments to identify designated information of varying sensitivity, i.e. "A" for low sensitivity, "B" for particularly sensitive information, and "C" for extremely sensitive. However, the security markings of PROTECTED and PROTECTED (SENSITIVE) **will continue to be used by EAITC** for information designated sensitive, but not in the national interest.

Note 1 – The sticker, form EXT 106, will need to be **fully completed** with the appropriate transmittal information for the classification categories of SECRET, CONFIDENTIAL, and PROTECTED (SENSITIVE), or if the addressee is preceded by the warning term "TO BE OPENED ONLY BY". The transmittal information is not normally required for all other categories.

Note 2 – For **TOP SECRET** documents, refer to the Manual of Security Instructions (MSI), and contact Special Records Unit/MIRD.

EXT 1512 (05/90)

ANNEX B

External Affairs and International Trade Canada | Affaires extérieures et Commerce extérieur Canada

DOCUMENT SECURITY WITHIN N.C.R. REFERENCE CHART

(Locations other than Lester B. Pearson Building)

Destination	1) PROTECTED * 2) PROTECTED "A"	1) CONFIDENTIAL 2) PROTECTED (SENSITIVE) * 3) PROTECTED "B" * 4) PROTECTED "C"	SECRET
Within Satellite Location	– one gum-sealed envelope affixed with sticker EXT 106	– one gum-sealed envelope affixed with sticker EXT 106	– one gum-sealed envelope affixed with sticker EXT 106
Within National Capital Region **including** Lester B. Pearson Building	– one gum-sealed envelope **without** security marking – first class mail, or pickup by MIRM messenger	– one gum-sealed envelope – security marking on upper upper right-hand corner of envelope – Division symbol and **"by-hand"** number on lower left-hand corner of envelope – close envelope with approved tape – pickup by MIRM messenger	– one gum-sealed envelope – enclose receipt form EXT 34 with document – security marking on upper right-hand corner of envelope – Division symbol and **"by-hand"** number on lower lower left-hand corner of envelope – close envelope with approved tape – pickup by MIRM messenger
Diplomatic Missions via MIRM	– enclose in special envelope EXT 2 or EXT 3 annotated with security marking and document number – pickup by MIRM messenger	– enclose in special envelope EXT 2 or EXT 3 annotated with security marking and document number – close envelope with approved tape – pickup by MIRM messenger	– enclose in special envelope EXT 2 or EXT 3 annotated with security marking and document number – close envelope with approved tape – pickup by MIRM messenger
Elsewhere in Canada	– one gum-sealed envelope **without** security marking – first class mail, or pickup by MIRM messenger	– prepare **two** gum-sealed envelopes, each with complete address of sender and receiver – security marking on upper right-hand corner of **inner** envelope – close inner envelope with approved tape – print **"Security Mail"** on upper right-hand corner corner of **outer** envelope – pickup by MIRM messenger	– prepare **two** gum-sealed envelopes, each with complete address of sender and receiver – enclose receipt form EXT 34 with document in inner envelope – security marking on upper right-hand corner of **inner** envelope – close inner envelope with with approved tape – print **"Security Mail"** on upper right-hand corner of **outer** envelope – pickup by MIRM messenger

* The categories of PROTECTED "A", "B", and "C" have been adopted by some other government departments to identify designated information of varying sensitivity, i.e. "A" for low sensitivity, "B" for particularly sensitive information, and "C" for extremely sensitive. However, the security markings of PROTECTED and PROTECTED (SENSITIVE) **will continue to be used by EAITC** for information designated sensitive, but not in the national interest.

Note 1 – The sticker, form EXT 106, will need to be **fully completed** with the appropriate transmittal information for the classification categories of SECRET, CONFIDENTIAL, and PROTECTED (SENSITIVE), or if the addressee is preceded by the warning term "TO BE OPENED ONLY BY". The transmittal information is not normally required for all other categories.

Note 2 – For **TOP SECRET** documents, refer to the Manual of Security Instructions (MSI), and contact Special Records Unit/MIRD.

EXT 1512-1 (05/90)

NOTES

NOTES