LA SÉCURITÉ ET LES *Mesures* DE PROTECTION

au Ministère des Affaires étrangères et du Commerce international

NUMÉROS DE TÉLÉPHONE IMPORTANTS

EN CAS D'URGENCE	992-1150 (Centre de contrôle des mesures d'urgence)
Vous avez besoin d'une nouvelle clé, d'un nouveau cadenas à combinaison ou à clé ?	992-6678 (Atelier de serrurerie d'ISRG)
Vous avez besoin d'information sur la destruction de renseignements de nature délicate ?	992-5452 (Atelier de serrurerie d'ISRG)
Vous avez besoin d'une carte d'identité, d'un laissez-passer ou d'un laissez-passer temporaire ?	(Section de l'identité d'ISRG) 996-8457 (SERV) 992-6691 (BG-180)
Vous ne pouvez entrer dans votre bureau fermé à clé ?	992-6678 (Atelier de serrurerie d'ISRG)
Vous avez perdu quelque chose ?	944-0019 (ISRG)
Vous avez besoin d'information sur les cours, les séminaires, les séances d'information ou les outils de travail sur la sécurité ?	992-6704 (ISDT)

Septembre 1998

Table des matières

À PROPOS DU PRÉSENT DOCUMENT

Le présent guide a pour objectif de vous aider à vous acquitter de vos responsabilités en matière de sécurité à titre d'employé du ministère des Affaires étrangères et du Commerce international (MAECI).

Depuis la manipulation, l'entreposage et la transmission de renseignements de nature délicate jusqu'à leur destruction, en passant par l'utilisation d'équipement protégé et l'accès aux zones de sécurité, la sécurité constituera un élément primordial de vos décisions quotidiennes. Vos responsabilités à ce chapitre prennent naissance dès votre arrivée au travail et se poursuivront même après que vous aurez quitté le Ministère.

Servez-vous du présent manuel comme outil de référence..

Certaines dispositions du présent guide, aussi bien en ce qui concerne la sécurité physique que les procédures en cas d'urgence, s'appliquent spécifiquement à l'édifice Lester B. Pearson à Ottawa. Si vous travaillez dans un autre édifice à Ottawa ou ailleurs au Canada, y compris sur les lieux d'un congrès, vous devriez connaître les mesures de sécurité et d'urgence qui y sont en vigueur. Certains renseignements concernent aussi les missions à l'étranger.

Étant donné que le présent guide contient seulement les grandes lignes des procédures qui touchent l'Administration centrale (édifice LBP), il n'est pas censé remplacer les instructions et politiques plus vastes sur la sécurité que publie le Ministère. Vous êtes invité à vous reporter à l'ensemble complet de politiques, procédures, conseils et directives qui sont à votre disposition. Pour de plus amples informations, consultez le Manuel des instructions de sécurité (MIS), la section appropriée de la Direction générale de la sécurité et du renseignement (ISD) ou la Section des opérations de sécurité (ISRG).

Si vous ne trouvez pas réponse à toutes vos questions dans le présent guide, ISDT offre des cours et des séances d'information en fonction des demandes dans les directions, les sections ou les directions générales. Communiquez avec la Section du personnel et de l'éducation en matière de sécurité (ISDT) au 992-6704 pour obtenir le calendrier des cours, qui liste les séances d'information offertes.

INTRODUCTION

Le ministère des Affaires étrangères et du Commerce international (MAECI) est un cas tout à fait unique parmi les divers ministères fédéraux, tant à cause de son cadre de travail que de son mandat.

En effet, chaque jour, le Ministère traite un fort volume de correspondance et de renseignements, dont une bonne partie sont de nature délicate. Il s'agit notamment d'informations qui émanent de gouvernements étrangers, d'autres ministères, d'entreprises et de l'industrie, ou de particuliers. Il est vital qu'elles soient protégées.

Le Ministère possède également des biens de valeur et possède ou loue à bail des chancelleries ou des résidences officielles, y compris des logements du personnel, des véhicules, des oeuvres d'art et du matériel de bureau qui valent des millions de dollars. De plus, bon nombre de missions génèrent des montants substantiels en espèces de même que des documents de voyage comme des passeports, des visas et des permis ministériels qui doivent être protégés.

Les programmes du Canada à l'étranger peuvent aussi être mis en péril : les programmes d'exportation représentent un volet fondamental de l'économie canadienne, de sorte que la perte d'une vente importante ou d'un gros marché d'exportation par suite d'une infraction à la sécurité est susceptible d'avoir de graves répercussions sur l'économie canadienne.

Bien que souvent difficile à quantifier, mais toujours critique pour une nation comme le Canada, il reste toute la dimension intangible de l'État. Le Canada doit garder la confiance des autres États pour que l'information puisse circuler librement. Il a aussi besoin de préserver son accès aux décideurs et son influence auprès d'eux. Il faut donc prendre soin d'éviter tout ce qui peut miner sa crédibilité sur le plan de la sécurité.

La préoccupation du Ministère pour la sécurité des employés et des personnes dont ils ont la charge (qui vivent et travaillent à l'étranger dans des conditions très diverses et souvent beaucoup plus dangereuses que celles d'Ottawa) est l'un des principaux éléments qui distinguent la politique de sécurité du MAECI de celle des autres ministères et organismes canadiens, où l'on met surtout l'accent sur les questions de sécurité de l'information.

> *REMARQUE* : Les procédures de sécurité occasionnent parfois des dérangements, mais il suffit souvent d'un peu de bon sens et de prévoyance pour assurer la sécurité de l'information et des biens matériels et votre propre sûreté.

QUE FAIRE EN CAS D'URGENCE ?

ISRG est responsable de la définition et de la mise en oeuvre de toutes les procédures, directives et instructions pour toute situation où sont en jeu soit la sécurité, soit la protection du personnel ou encore de renseignements et de biens de nature délicate à l'édifice LBP. Il incombe également à ISRG de former les employés et de veiller au respect des directives permanentes à l'intention des gardes de sécurité en situation d'urgence, en cas de risque d'incendie, d'alerte à la bombe, de manifestation ou d'autres troubles.

QUELLES SONT LES CONSIGNES D'URGENCE À L'ÉDIFICE ?

Des procédures simples en cas d'urgence ont été définies pour l'édifice LBP et sont consignées dans le Manuel des instructions de sécurité de même que dans le livret intitulé « Procédures d'urgence - Édifice Lester B. Pearson ». Elles vous permettent de réagir de manière rapide, coordonnée et efficace dans diverses situations d'urgence au travail, que ce soit un incendie, une urgence médicale ou une urgence grave touchant l'édifice.

Prenez le temps de lire et d'assimiler ces procédures.

QU'EST-CE QUE LE CENTRE DE CONTRÔLE DES MESURES D'URGENCE DE L'ÉDIFICE PEARSON ?

Le Centre de contrôle des mesures d'urgence surveille toutes les alarmes de sécurité et d'incendie de l'édifice LBP de même que le réseau de téléphones rouges d'urgence. Situé au rez-de-chaussée de la tour B, le centre est en activité 24 heures sur 24; son personnel bilingue est constitué de membres spécialement formés du Corps canadien des commissionnaires qui connaissent tous les aspects de l'édifice. Les commissionnaires peuvent communiquer dans tout l'édifice durant les heures normales de travail et en dehors. Le système de communication vocale est géré à partir du centre et compte plus de 100 téléphones rouges d'urgence disséminés dans l'édifice. Le centre possède en outre des jeux complets des plans d'étage et des clés de l'édifice.

Si le personnel du centre est avisé d'une urgence, il communique avec tous les services d'intervention requis en cas d'urgence :

- Services régionaux et municipaux d'intervention d'urgence; et
- Organisation des services de secours de l'édifice.

QUI SONT LES AGENTS DE SECOURS D'ÉTAGE ?

Chaque étage est doté d'agents de secours qui savent comment donner de l'aide et communiquer des directives en cas d'urgence. Une liste du personnel de secours affecté à votre étage est affichée près des escaliers de secours. Vous devriez apprendre le nom de ces agents, savoir où ils travaillent et connaître leur numéro de téléphone. Durant une urgence, les agents de secours portent un casque de protection.

QUE FAIRE EN CAS D'URGENCE ?

Dans l'éventualité d'un incendie, d'une urgence médicale, d'une alerte à la bombe, d'un crime, de troubles, d'une intrusion, d'une défaillance de l'édifice ou de l'équipement, d'une catastrophe naturelle, communiquez avec le Centre de contrôle des mesures d'urgence, soit en utilisant la ligne directe des téléphones rouges d'urgence soit en composant le 992-1150, ou actionnez l'avertisseur d'incendie.

ET SI MA MOBILITÉ EST RÉDUITE ?

Si votre mobilité est réduite ou que vous avez un handicap sensoriel, ou encore si vous êtes temporairement invalide en raison d'une blessure ou d'un problème médical, faites-le savoir à une ou plusieurs personnes qui accepteront d'être vos surveillants personnels, à l'agent de secours d'étage et au Centre de contrôle des mesures d'urgence. Ainsi, ce dernier pourra gérer la situation en toute sécurité. Si vous ne souhaitez pas parler de votre état, faites au moins savoir à l'agent de secours d'étage que vous pourriez avoir besoin d'aide en cas d'évacuation d'urgence.

QUE FAIRE S'IL Y A UN INCENDIE ?

Si vous découvrez un incendie ou si vous décelez de la fumée ou une odeur de gaz :

- actionnez l'avertisseur d'incendie le plus proche;
- évacuez immédiatement les lieux en empruntant l'escalier le plus proche;
- une fois dehors, tenez-vous à au moins 100 mètres (300 pieds) de l'édifice.

Si vous entendez une alerte (une sonnerie de 20 battements à la minute) :

- écoutez les instructions données par le système de sonorisation de secours;
- préparez-vous à évacuer les lieux lorsqu'on vous l'ordonnera.

Si vous entendez un signal d'alarme (une sonnerie de 120 battements à la minute) :

- écoutez et suivez les instructions données par le système de sonorisation de secours;
- évacuez immédiatement les lieux lorsqu'on vous l'ordonnera en empruntant l'escalier le plus proche;
- n'essayez pas de sortir votre véhicule du garage

Les personnes ayant une mobilité réduite doivent attendre les instructions et l'aide de leurs agents de secours d'étage en cas d'incendie, qui peuvent donner les premiers soins, connaissent les procédures d'urgence et d'incendie, savent se servir des extincteurs et sont au courant des mesures d'évacuation et de réaction en cas d'urgence.

Les consignes d'incendie sont affichées dans les vestibules des ascenseurs et à d'autres endroits stratégiques tels que les entrées des tours. Vous devriez les lire, savoir où se trouve l'équipement de secours et connaître les chemins d'évacuation en cas d'incendie.

COMMENT RÉAGIR EN CAS D'ALERTE À LA BOMBE ?

En cas d'alerte à la bombe, ou si un objet ou un paquet suspect est trouvé, ne touchez à rien, mais appelez immédiatement le Centre de contrôle des mesures d'urgence. Il est important de donner le plus de détails possible sur l'incident pour que la haute direction puisse prendre les décisions appropriées concernant les mesures à mettre en œuvre.

Pour de plus amples renseignements, reportez-vous aux *Mesures d'urgence, Guide de l'employé* et à la brochure de la GRC *Appels à la bombe, feuille de contrôle*. Ces publications sont disponibles à l'entrée des tours, au niveau du hall principal et à l'étage inférieur.

QUE FAIRE EN CAS DE MANIFESTATION ?

L'édifice LBP peut être la cible d'une manifestation ou d'une occupation après entrée non autorisée ou prise de possession par la force. Le cas échéant, prenez les précautions suivantes :

- n'intervenez pas personnellement et n'essayez pas d'interrompre la manifestation quelle qu'elle soit;
- n'encouragez pas les participants et ne discutez pas non plus avec eux;
- ne vous mettez pas dans une position où vous risqueriez d'être pris en otage;
- n'essayez pas de protéger des documents de nature délicate si vous êtes en situation de risque;
- conseillez et appuyez vos collègues qui cherchent à éviter la confrontation;
- observez les gestes des manifestants et cherchez à les identifier.

QUE DOIS-JE FAIRE EN CAS DE PERTE OU DE VOL ?

Protégez vos biens personnels en gardant en tout temps votre sac à main, votre portefeuille, votre argent et vos objets qui ont une valeur sentimentale sur vous ou en sécurité. N'oubliez pas que les tiroirs de votre bureau ne sont pas un lieu sûr.

N'oubliez pas non plus qu'il vous incombe de protéger les biens du gouvernement qui sont intéressants pour les voleurs, comme les calculatrices, les ordinateurs (surtout les ordinateurs portatifs ou bloc-notes), les magnétophones ou les caméras : placez-les dans un classeur ou une pièce fermés à clé lorsque vous ne les utilisez pas.

En cas de perte ou de vol, communiquez avec ISRG (Opérations de sécurité), au 944-0019. Vous devez également signaler la perte d'un bien du gouvernement à SBAD (Gestion des registres d'inventaire), au 996-6816 et à SBRP (Politique financière ministérielle, Formation et rapports) au 994-1102.

QU'EST-CE QUE LA SÉCURITÉ DE L'INFORMATION ?

La Politique du gouvernement sur la sécurité établit un cadre de directives concernant le respect des exigences en matière de sécurité et de protection des renseignements personnels. Ce cadre oblige le Ministère à protéger de façon adéquate les informations personnelles et autres données de nature délicate contenues dans ses systèmes d'information ou utilisés pour la prestation de ses programmes et services. La politique est fondée sur le principe selon lequel les méthodes de protection de l'information et des biens devraient clairement refléter leur niveau de confidentialité, leur importance et leur valeur — ni plus, ni moins.

Votre responsabilité consiste à protéger les renseignements et les biens de nature délicate que vous devez utiliser dans votre travail quotidien contre toute divulgation, destruction, élimination ou modification non autorisées. Personne ne veut, en compromettant des renseignements, mettre en danger l'intérêt national ou d'autres intérêts dont le Parlement assume la responsabilité.

Dans vos activités de tous les jours, assurez-vous que vous êtes en mesure :

- ✔ de déterminer quels renseignements sont de nature délicate;
- ✔ de choisir le niveau de confidentialité approprié pour les renseignements que vous produisez;
- ✔ de marquer de façon adéquate ces renseignements afin que les tiers sachent qu'il faut appliquer des mesures de protection spéciales.

Vous devriez également pouvoir :

- ✔ choisir de l'équipement protégé et un emplacement sûr pour produire de tels renseignements, en discuter ou les transmettre;
- ✔ stocker l'information de façon sûre;
- ✔ détruire l'information de façon sûre.

QU'EST-CE QU'UN RENSEIGNEMENT DE NATURE DÉLICATE ?

Tous les rensignements n'ont pas à être classifiés ou désignés. Cependant, les ren-

seignements et les biens du Ministère doivent au moins faire l'objet d'une attention raisonnable qui est conforme aux pratiques administratives de base. En tout cas, il ne faut jamais classifier ou désigner des renseignements afin de dissimuler des infractions à la loi, des lacunes ou des erreurs administratives, ou encore afin d'éviter des embarras ou de limiter la concurrence.

Toutefois, il est vrai que certains renseignements et biens sont plus confidentiels ou précieux que d'autres, et doivent donc faire l'objet de mesures de protection plus strictes. 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, il vous incombe de préciser la classification et désignation des renseignements que vous produisez.

Le Guide de classification et de désignation du Ministère précise les directives à suivre en matière de classification; ce document est disponible par le biais de l'Intranet du MAECI. Vous pouvez également communiquer avec ISC pour plus d'information.

Il existe trois niveaux de confidentialité : non classifié, désigné et classifié.

EXEMPLES DE RENSEIGNEMENTS CLASSIFIÉS

TRÈS SECRET

- Information sur un risque de conflit armé contre le Canada ou ses alliés
- Information sur les méthodes et les opérations fructueuses des services de renseignement et de contre-espionnage nationaux
- Rapports dont la diffusion pourrait entraîner la mort ou la torture d'une personne dont le maintien en vie est dans l'intérêt national

SECRET

- Procès-verbaux des réunions du Cabinet ou des comités du Cabinet
- Rapports sur d'importantes négociations internationales
- Rapports scientifiques ou techniques ayant trait à la défense ou à la sécurité nationale

CONFIDENTIEL

- Dossiers sur les discussions des comités interministériels
- Instructions sur la protection de renseignements très confidentiels
- Rapports des missions ou du Canada qui peuvent profiter à des nations étrangères ou nuire aux relations internationales

EXEMPLES DE RENSEIGNEMENTS DÉSIGNÉS

PROTÉGÉ C

- Rapports dont la diffusion pourrait compromettre la sécurité d'une personne
- Rapports contenant des renseignements commerciaux d'une importance critique

PROTÉGÉ B

- Comptes rendus de discussions visés par le secret professionnel de l'avocat
- Rapports sur la situation financière d'une entreprise
- Rapport d'évaluation complet

PROTÉGÉ A

- Salaire exact d'un employé
- Numéro d'assurance sociale

REMARQUE : N'oubliez pas de toujours marquer adéquatement les renseignements que vous produisez.

EXTRACTION DE RENSEIGNEMENTS CLASSIFIÉS

Les renseignements extraits d'un document déjà classifié ou désigné sont automatiquement classifiés ou désignés en fonction du document d'où ils sont tirés. Par exemple, l'auteur d'une note d'information sur un document classé SECRET doit attribuer à sa note la classification SECRET.

- bibliographies et sources
- tableaux et cartes
- films et négatifs
- chemises de dossiers
- formulaires
- documents de l'OTAN
- documents utilisés à l'externe
- documents portant une mention descriptive

DÉCLASSIFICATION OU DÉCLASSEMENT AUTOMATIQUE

Les renseignements ne sont classifiés ou désignés que pour la période pendant laquelle ils doivent être protégés. Après cette période, la classification ou la désignation doit être supprimée ou abaissée. Lorsque vous créez un document, vous pouvez préciser la date ou l'événement après lequel le document peut être automatiquement déclassifié ou déclassé.

Exemples :

1. Confidentiel (non classifié après le 31 juillet 1999)
2. Protégé A (non classifié si l'annexe A est retirée)

MODIFICATION DE LA CLASSIFICATION OU DE LA DÉSIGNATION D'UN DOCUMENT

Si vous voulez modifier la classification ou la désignation d'un document, vous devez :

- être l'auteur du document, ou son remplaçant;
- avoir un lien de responsabilité clair relativement à l'information;
- avoir une connaissance approfondie de l'information et de son caractère délicat.

La date, le responsable et la nouvelle classification ou désignation doivent être inscrits lisiblement à l'encre sur le document ou le bien.

Vous devez faire tout votre possible pour obtenir la participation de l'auteur du document avant de modifier sa classification ou sa désignation, mais il arrive que l'information soit déclassifiée et mise en circulation sans la participation de l'auteur ou sans qu'il en ait connaissance. (Par ex., demandes en vertu de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels.)

Si une classification ou désignation est supprimée ou abaissée, cela ne signifie pas que l'information peut ou doit être communiquée au public. Les demandes d'information du public, des médias, de l'industrie, etc., doivent être transmises au Service des relations avec les médias (BCM) ou au bureau du Coordonnateur de l'accès à l'information et de la protection des renseignements personnels (JIP).

SÉCURITÉ DU PERSONNEL

QUI PEUT AVOIR ACCÈS À DES RENSEIGNEMENTS DE NATURE DÉLICATE ?

Un des principes fondamentaux et importants de la sécurité est celui de l'accès sélectif. Il s'agit en fait de limiter l'accès aux renseignements désignés ou classifiés aux personnes qui en ont besoin pour effectuer leur travail. Aucun employé n'a le droit de prendre connaissance ou de conserver des renseignements classifiés simplement parce qu'il détient une autorisation de sécurité d'un niveau donné.

À l'instar des autres employés du Ministère, vous avez dû vous soumettre au processus de contrôle de sécurité avant d'être nommé à votre poste :

Il existe deux types de vérification de sécurité :

- vérification approfondie de la fiabilité (VAF) ou vérification de base de la fiabilité (VBF)
- évaluation des habilitations de sécurité

REMARQUE : pour avoir accès au secteur d'opérations de l'édifice L. B. Pearson, il faut une autorisation de niveau SECRET.

QU'EST-CE QUE LA VÉRIFICATION APPROFONDIE OU DE BASE DE LA FIABILITÉ ?

Cette vérification doit être menée par le gestionnaire responsable de l'embauche, l'agent de dotation ou l'agent administratif avant qu'une autorisation de sécurité puisse être demandée et avant la nomination d'un employé. Une fois que vous obtenez cette autorisation, vous pouvez avoir accès à des renseignements et des biens non classifiés et désignés.

Ces vérifications portent sur les éléments suivants :

- renseignements de nature personnelle et professionnelle;
- études et qualifications professionnelles;
- accréditations ou certifications;
- références;

- casier judiciaire;
- cote de solvabilité;
- répertoire du SCRS

Une fois la VAF effectuée, on peut avoir accès aux renseignements désignés (protégé A, B et C).

QU'EST-CE QU'UNE ÉVALUATION POUR AUTORISATION DE SÉCURITÉ ?

L'évaluation pour autorisation de sécurité est requise pour toute personne qui a accès à des renseignements ou à des biens classifiés, quel que soit le type d'affectation qui lui est confiée. Cette évaluation s'ajoute à la vérification approfondie ou de base de la fiabilité. Elle porte sur :

- les références concernant votre réputation;
- vos antécédents personnels, pouvant couvrir une période de dix ans ou plus;
- les répertoires du Service canadien du renseignement de sécurité (SCRS);

Il existe trois niveaux d'autorisation de sécurité, qui correspondent aux trois niveaux de documents classifiés :

Niveau I	- accès aux documents CONFIDENTIELS
Niveau II	- accès aux documents SECRETS
Niveau III	- accès aux documents TRÈS SECRETS

Une autorisation de niveau II - SECRET est une exigence minimale pour travailler au Ministère.

Une autorisation de niveau III - TRÈS SECRET est une exigence minimale pour les membres permutants du service extérieur affectés à l'étranger.Niveau III - accès aux documents TRÈS SECRETS

À retenir :

✔ L'autorisation de sécurité est obligatoire, que vous soyez un employé à temps plein, temporaire ou contractuel.

- ✔ Le niveau de votre autorisation de sécurité peut être mis à jour au besoin, et DOIT l'être tous les cinq ans pour une autorisation de niveau III et tous les dix ans pour les autorisations de niveau I et II.
- ✔ Votre niveau d'autorisation de sécurité est transférable si vous passez d'un poste à un autre au sein du Ministère, si vous travaillez sous contrat pour un autre ministère, ou encore si vous êtes détaché ou muté dans un autre ministère.

MARIAGE OU COHABITATION

Si vous détenez une autorisation de sécurité valide et avez l'intention de vous marier ou de cohabiter avec quelqu'un (y compris une personne du même sexe), vous devez remplir le formulaire EXT 332 Avis de projet de mariage ou de cohabitation et le soumettre à ISDT pour vérification. D'après les renseignements que vous aurez fournis, une évaluation de sécurité sera menée. Cette évaluation n'est pas la même que celle employée pour octroyer une autorisation de sécurité.

LORSQUE VOUS QUITTEZ LE MINISTÈRE

Les gestionnaires et les agents de dotation doivent remplir le formulaire Annulation de la vérification de fiabilité approfondie/Autorisation de sécurité pour des raisons administratives - TBS/SCT 330-25 pour chaque employé quittant le Ministère. Le formulaire doit être expédié à ISDT au mois deux semaines avant la cessation de l'emploi.

RÉVOCATION OU ABAISSEMENT DE LA COTE DE FIABILITÉ OU DE L'AUTORISATION DE SÉCURITÉ

À la suite d'une mise à jour ou d'une révision fondée sur des renseignements défavorables concernant une personne, celle-ci peut se voir retirer sa cote de fiabilité ou son autorisation de sécurité.

Le pouvoir de refuser, révoquer ou suspendre les autorisations de sécurité appartient au sous-ministre, qui ne peut pas le déléguer.

Le pouvoir de refuser, révoquer ou suspendre les cotes de fiabilité incombe au gestionnaire compétent.

Dans les deux cas, l'intéressé est informé de son droit d'examen et de recours et privé de l'accès aux renseignements et biens sensibles. Lorsque l'intéressé est informé des raisons du refus, il est aussi avisé de son droit de recours.

QU'EST-CE QUE LA SÉCURITÉ PHYSIQUE ?

La sécurité physique comprend toutes les mesures prises pour protéger les renseignements et les biens de nature délicate de même que pour garantir la sécurité du personnel, notamment :

- surveillance quotidienne des entrées et sorties à l'édifice Lester B. Pearson;
- cartes d'identité et laissez-passer donnant accès à l'édifice;
- surveillance par télévision en circuit fermé des points d'entrée et de sortie;
- armoires métalliques de sûreté et classeurs approuvés;
- chambres fortes;
- déchiqueteuses approuvées;
- systèmes d'alarme et équipement connexe;
- contrôle radioscopique du courrier;
- systèmes de contrôle de l'accès et de détection des intrusions, et secteurs de réception et d'opérations, zones de sécurité et de haute sécurité.

OÙ SE TROUVENT LES SECTEURS À ACCÈS RESTREINT ?

Tous les lieux occupés en partie ou en totalité par le Ministère sont divisés en secteurs à accès restreints. On vise ainsi à contrôler l'accès, à protéger tous les biens du gouvernement et à garantir la sécurité de son personnel.

Secteurs ouverts au public
Ces secteurs entourent toutes les installations, ou en font partie. Par exemple, dans l'édifice LBP, la cafétéria, la Banque Royale et le hall sont des secteurs ouverts au public.

Réception
Situé à l'entrée de l'édifice, ce secteur constitue le premier point de contact entre le public et le Ministère. Il s'agit également de l'endroit où certains services sont fournis, où les renseignements sont transmis et où l'accès aux zones d'accès restreint est contrôlé. Le Centre des services (SERV) de l'édifice LBP en est un bon exemple.

Secteurs des opérations
L'accès à ces secteurs est limité au personnel et aux visiteurs qui sont escortés par des employés détenant une autorisation de sécurité. Toutes les tours de l'édifice LBP sont des secteurs d'opérations.

Zones de sécurité

L'accès à ces zones est limité au personnel autorisé et aux visiteurs qui sont escortés par des employés détenant une autorisation de sécurité. Ces zones sont surveillées en tout temps par des agents de sécurité, d'autres employés ou par des systèmes électroniques.

Zones de haute sécurité

L'accès à ces zones est contrôlé par des points d'entrée. Il est limité au personnel détenant l'autorisation appropriée et aux visiteurs qui sont escortés par des employés détenant une autorisation de sécurité. Ces zones sont surveillées en tout temps par des agents de sécurité, d'autres employés ou par des systèmes électroniques.

9e étage de la tour A :

Il s'agit d'une zone où se tiennent les réceptions, conférences et banquets du Ministère; les visiteurs doivent être escortés dans tous leurs déplacements en direction et en provenance du 9e étage de la tour A. Ils n'ont pas accès sans escorte aux autres étages de la tour A ou aux autres tours.

COMMENT PUIS-JE ACCÉDER À UN SECTEUR RESTREINT ?

Des lecteurs de cartes magnétiques sont installés à l'entrée de chaque tour. Des laissez-passer ministériels et temporaires de trois couleurs différentes permettent d'accéder à l'édifice LBP.

Laissez-passer bleu :

Ce laissez-passer vous permet d'accéder aux zones d'accès restreint 24 heures par jour, 7 jours par semaine. Il vous permet également d'escorter des visiteurs ou des employés qui n'ont pas de laissez-passer pour les zones d'accès restreint de l'édifice abritant les bureaux du Ministère. Pour obtenir un laissez-passer bleu, il faut détenir au moins une autorisation de sécurité de niveau II (SECRET).

Laissez-passer vert :

Ce laissez-passer vous permet de pénétrer dans les secteurs d'accès restreint pendant les heures normales de travail, soit de 7 h à 18 h, du lundi au vendredi, sauf les jours fériés. Ce laissez-passer ne vous permet pas d'escorter des visiteurs sur les lieux. Il faut au moins disposer d'une autorisation de sécurité de niveau II (SECRET) pour obtenir ce laissez-passer.

Laissez-passer rouge :
Le laissez-passer rouge est délivré au personnel qui n'a habituellement pas besoin d'accéder aux zones d'accès restreint, ou qui ne dispose pas au moins d'une autorisation de sécurité SECRET. Avec un laissez-passer rouge, vous devez être escorté dans les secteurs d'accès restreint.

Laissez-passer temporaire :
Un laissez-passer temporaire ne vous est remis que si vous disposez déjà d'un laissez-passer bleu ou vert et que vous l'avez oublié ou perdu. Votre laissez-passer initial est désactivé lorsque vous demandez le laissez-passer temporaire et réactivé lorsque vous remettez ce dernier.

Si vous êtes muté ou que vous quittez votre emploi, vous devez rendre votre laissez-passer. Si vous le perdez, communiquez immédiatement avec la Section de l'identité ISRG.

Centre des services (SERV)	996-8457
Section de l'identité (BG-180)	996-6691

N'oubliez pas qu'il est de votre responsabilité de vous assurer que quiconque entre dans une tour immédiatement après vous est autorisé à le faire.

COMMENT PUIS-JE OBTENIR UN LAISSEZ-PASSER ?

Ils sont délivrés par ISRG à deux endroits : le Centre des services (SERV) situé dans le hall principal (8 h 30 à 11 h 30 et 13 h à 14 h 30) et à la section de l'identité ISRG, qui est située au BG-180 (7 h à 16 h).

ACCÈS DES VISITEURS

Les visiteurs qui veulent se rendre dans une zone à accès restreint doivent être escortés en tout temps. Le non-respect de cette exigence peut constituer une infraction à la sécurité.

Une fois la visite terminée, il vous incombe d'escorter ces visiteurs vers une zone publique ou de faire en sorte qu'une personne les escorte vers cette zone. Cela vaut aussi pour les personnes de l'extérieur qui participent à des réunions à l'édifice L.B. Pearson.

QUE FAUT-IL FAIRE POUR SE RENDRE DANS UNE ZONE À ACCÈS RESTREINT EN DEHORS DES HEURES NORMALES DE TRAVAIL (SUR SEMAINE ENTRE 16 H ET 8 H, LES FINS DE SEMAINE ET LES JOURS DE CONGÉ) ?

Même s'il existe des lecteurs de cartes magnétiques, il est obligatoire de signer le registre à votre entrée dans l'édifice LBP et à votre sortie en dehors de heures de travail. C'est un moyen de savoir quels sont les employés qui sont dans l'édifice et l'endroit où ils se trouvent en cas d'urgence, notamment d'incendie.

QU'EN EST-IL DES SYSTÈMES D'ALARME ?

Les portes de contrôle d'accès situées à l'entrée des tours de l'édifice LBP sont protégées par des systèmes d'alarme qui peuvent être activés pendant les heures à accès limité. Si vous voulez entrer dans un secteur à accès restreint durant ces périodes, faites-en la demande au commissionnaire de service. Si vous tentez d'entrer dans tout autre secteur à accès restreint pendant ces périodes, vous pourriez déclencher le système d'alarme, ce qui donnera lieu à une intervention des services de sécurité.

QUEL EST LE RÔLE DES SERVICES DE SÉCURITÉ CONCERNANT LE STATIONNEMENT ?

Les permis de stationnement sont délivrés par la Direction des services administratifs à l'administration centrale (SBA), située au rez-de-chaussée de la tour A de l'édifice LBP. Si vous avez des questions concernant ces permis, communiquez avec SBAA (992-2338). ISRG, par un accord spécial avec la GRC, applique les règlements sur le stationnement établis dans la Loi relative à la circulation sur les terrains de l'État.

QUELLES SONT LES RESPONSABILITÉS DU CORPS CANADIEN DES COMMISSIONNAIRES ?

Le Corps canadien des commissionnaires assure des services de sécurité pour l'édifice LBP. Ces commissionnaires peuvent exiger la présentation de cartes d'identité. Ils sont chargés :

- d'assurer la réception et de contrôler l'accès;
- de contrôler les systèmes d'alarme de l'édifice et d'intervenir, au besoin;
- de mener des patrouilles de sécurité et des rondes d'incendie;
- de contrôler l'entrée des visiteurs et de les escorter jusqu'au bureau d'un employé après avoir communiqué avec ce dernier.
- de surveiller le matériel qui entre dans l'édifice LPB et qui en sort.

COMMENT DOIS-JE TRAITER LES DOCUMENTS DE NATURE DÉLICATE ?

De nombreux documents entrent au Ministère ou en sortent. Certains sont de nature plus délicate que d'autres. Dans certains cas, les documents doivent être livrés « par porteur » pour que le contrôle soit ininterrompu. Dans d'autres cas, les documents peuvent être transmis par la poste ou par messager, pourvu qu'ils soient adéquatement enveloppés.

TRANSMISSION DE RENSEIGNEMENTS ET DE BIENS DE NATURE DÉLICATE (Voir L'appendice A aux pages 36 et 37).

TRANSPORT DE RENSEIGNEMENTS ET DE BIENS DE NATURE DÉLICATE (Voir L'appendice B aux pages 38 et 39).

QU'EST-CE QU'UN TÉLÉPHONE PROTÉGÉ?

Un téléphone protégé, appelé STU-III, fournit un moyen de communication téléphonique classifiée au personnel qui a besoin de transmettre des renseignements classifiés et sensibles ou d'en discuter. Le terminal STU-III peut être utilisé comme un téléphone ordinaire, raccordé directement au réseau téléphonique public. Il peut aussi servir en mode protégé lorsque le module cryptographique est activé et que le terminal communique avec un autre STU-III en passant par le réseau public. Les STU-III sont des pièces d'équipement de cryptographie contrôlées. Le terminal, pris isolément, est NON CLASSIFIÉ; la clé d'activation cryptographique (CAC), prise isolément, est aussi NON CLASSIFIÉE; une fois la clé insérée dans le terminal, cependant, l'appareil acquiert la classification de son usage cryptographique opérationnel classifié.

Les conditions suivantes sont des atteintes possibles à la sécurité et doivent être signalées immédiatement à ISDF :

- lorsqu'un terminal STU-III est perdu ou volé;
- lorsqu'une CAC est perdue ou volée;
- lorsqu'une CAC a été laissée dans un terminal sans surveillance, on considère ordinairement qu'il y a eu infraction à la sécurité avec atteinte possible;
- lorsqu'un STU-III semble avoir été soumise à des interventions abusives.

QU'EST-CE QU'UN TÉLÉCOPIEUR PROTÉGÉ ?

L'équipement nécessaire à la transmission protégée de documents (jusqu'au niveau SECRET) par télécopieur est disponible dans de nombreux bureaux. Les contrôles sont similaires à ceux employés pour les téléphones STU III; si vous êtes autorisé à utiliser cet équipement, on vous indiquera comment vous en servir.

Ne présumez jamais que les téléphones, les téléphones cellulaires, les téléphones dans les véhicules, les télécopieurs, le courrier électronique ou tout autre mode de transmission électronique sont protégés.

N'utilisez jamais un de ces modes de transmission pour envoyer des renseignements de nature délicate.

COMMENT DOIS-JE RANGER LE MATÉRIEL DE NATURE DÉLICATE ?

Vous devez assurer en TOUT temps la protection des renseignements classifiés ou désignés qui se trouvent en votre possession.

Lorsque vous vous absentez de votre bureau pour une période prolongée, verrouillez bien les portes et les fenêtres et rangez le matériel de nature délicate dans un classeur fermant à clé ou un coffre-fort approuvé de la manière indiquée plus loin.

Ce genre de matériel doit également être rangé en lieu sûr durant les pauses du midi, en dehors des heures normales de travail, les fins de semaine et les congés, ou lorsque vous vous absentez pour une longue période durant les heures normales de travail (sauf si le secteur est surveillé pendant toute votre absence par un autre membre du personnel qui possède une autorisation de sécurité).

PUIS-JE DISCUTER DE RENSEIGNEMENTS DE NATURE DÉLICATE ?

- Vous ne devez pas discuter de renseignements de nature délicate dans un endroit public ni sur une ligne téléphonique non protégée.
- Lorsque vous discutez de renseignements de nature délicate avec quelqu'un, assurez-vous que votre interlocuteur en connaît la classification ou la désignation.
- Dans le cas d'une conférence ou autre événement public, les participants doivent être informés de la nature délicate des sujets abordés au début et à la fin de l'événement.

- Vous pouvez discuter de renseignements de nature délicate si vous utilisez le réseau téléphonique protégé STU-III. Vous trouverez de plus amples informations dans le Manuel des instructions de sécurité.

QUELLES SONT LES EXIGENCES MINIMALES CONCERNANT LE RANGEMENT DU MATÉRIEL DE NATURE DÉLICATE ?

Les exigences minimales applicables au Canada sont les suivantes :

Très secret:
doit être rangé dans une armoire métallique de sûreté ou un classeur de sûreté dans une zone de haute sécurité

Confidentiel, Secret, Protégé A, B,C:
Peut être rangé dans un secteur des opérations mais dans un classeur de sûreté approuvé, muni d'un moraillon double et d'un cadenas à combinaison Sargent et Greenleaf (S&G) approuvé.

QUAND DOIT-ON DEMANDER UN CHANGEMENT DE COMBINAISON ?

Une combinaison doit être changée dans les cas suivants :

- lorsque la personne qui connaît la combinaison est mutée, qu'elle a quitté son emploi ou n'a plus besoin d'avoir accès à l'information;
- lorsque la combinaison est ou peut être compromise;
- au moins une fois par an.

QUELLES SONT LES EXIGENCES CONCERNANT LES CLÉS DES BUREAUX ?

La secrétaire ou la personne responsable des clés dans votre section vous remettra la clé de votre bureau. Vous devez rendre la clé à cette même personne lorsque vous n'occupez plus le bureau.

Si vous avez fermé votre bureau en laissant la clé à l'intérieur ou que vous avez oublié votre clé à la maison, vous devez demander à la secrétaire ou à la personne responsable des clés dans votre section d'ouvrir la porte. Si aucun d'eux n'est disponible, téléphonez à l'atelier de serrurerie d'ISRG (992-6678) pour faire ouvrir la porte. Le

délai d'intervention dépend de la disponibilité du personnel.

- Protégez vos clés en tout temps.
- Ne faites pas un double de vos clés; les clés de rechange sont contrôlées par les secrétaires de direction.
- La secrétaire peut obtenir une nouvelle clé en faisant parvenir un courrier électronique à l'atelier de serrurerie d'ISGR.

Une protection inadéquate des clés constitue un MANQUEMENT À LA SÉCURITÉ.

QU'EST-CE QU'UNE CARTE D'ABSENCE

On utilise les cartes d'absence pour empêcher que du matériel ou des documents classifiés et (ou) désignés soient livrés et laissés sur les bureaux lorsque les employés sont absents.

Si vous prévoyez vous absenter, demandez une carte d'absence à SBAM et placez-la sur votre bureau. Ne laissez jamais de matériel ou de documents classifiés et (ou) désignés sur votre bureau.

PUIS-JE EMPORTER DU MATÉRIEL DE NATURE DÉLICATE POUR TRAVAILLER À LA MAISON ?

Vous devez parfois travailler avec du matériel classifié et (ou) désigné le soir ou la fin de semaine, mais il est dangereux et interdit d'apporter ce genre de document à la maison ou à quelqu'autre endroit que ce soit. Dans certains cas, cependant, à Ottawa, le directeur peut en accorder la permission.

La permission peut être accordée aux conditions suivantes :

- il est interdit d'apporter des renseignements TRÈS SECRETS;
- vous êtes personnellement responsable de la garde du matériel;
- le matériel doit demeurer en votre possession en tout temps.

Personne ne peut sortir de l'équipement et du matériel (y compris du matériel et des logiciels informatiques) des bureaux du MAECI sans avoir d'abord rempli le formulaire GC 205 Autorisation de retirer du matériel de l'immeuble. On utilise également ce formulaire pour emporter des effets personnels qui peuvent sembler appartenir au gouvernement.

Comment détruire les renseignements de nature délicate ?

Les documents classifiés et désignés (Protégé B et C) doivent être éliminés à l'aide des destructeurs de documents qu'on trouve sur tous les étages de l'immeuble LBP. Si vous avez un volume important de documents de rebut classifiés (par exemple, si votre direction déménage), téléphonez à ISRG (992-5452) pour les faire ramasser.

Comment doit-on traiter les documents du Cabinet ?

Les documents du Cabinet sont distribués par porteur aux ministres, aux sous-ministres et aux employés qui doivent en prendre connaissance. Tous les documents du Cabinet « entrés » et « sortis », de même que le nom de l'agent responsable de leur sécurité sont consignés dans le registre PPDC. Un système de rappel est également en place, de sorte qu'un rappel est envoyé aux agents lorsque la date de retour est imminente.

Il vous incombe d'assurer la bonne garde et le retour des documents du Cabinet. Il n'est permis en aucun cas de copier ou de reproduire ces documents.

Que fait-on avec le matériel de nature délicate lorsqu'on quitte son emploi ?

Peu importe les circonstances dans lesquelles vous quittez votre emploi, il importe que vous compreniez et respectiez vos obligations en matière de sécurité. À votre départ, vous devez personnellement vider vos classeurs et autres meubles de rangement, et vous assurer qu'on n'enlève ni ne détruit par mégarde des dossiers, des disquettes ou d'autre matériel.

Les documents doivent être éliminés conformément à la Politique des Archives nationales et aux exigences de sécurité ministérielles.

Vous devez également :

- ✔ remettre à votre supérieur tous les documents contenant des renseignements classifiés, ainsi que tout autre bien du gouvernement obtenu durant votre période de service;
- ✔ rendre votre carte d'identité à la section de l'identité, salle BG-180, ou au centre de services, salle D1-425;
- ✔ remplir le formulaire TBS-SCT 330-25, Annulation de la vérification de fiabilité approfondie/autorisation de sécurité pour des raisons administratives.

perte ou du vol d'un équipement ou de matériel désigné ou classifié ou encore de dommages causés délibérément à cet équipement ou à ce matériel.

En cas d'infraction à la sécurité, avisez immédiatement votre superviseur et l'agent de sécurité du ministère (ISD). Il ne faut jamais tarder à le faire par crainte d'être mal à l'aise ou d'être tenu responsable, car un tel retard pourrait empirer les choses.

Un manquement à la sécurité survient lorsqu'on ne respecte pas les politiques et procédures de sécurité, ce qui risque d'occasionner une infraction à la sécurité. Il y a manquement dans les circonstances suivantes :

- Vous ne classifiez pas ou vous ne désignez pas certains renseignements conformément à la politique de sécurité;
- Des renseignements sont classifiés ou désignés en contravention à la politique de sécurité;
- Des renseignements ou des biens classifiés ou désignés sont modifiés, conservés, divulgués ou enlevés sans autorisation;
- Vous omettez de protéger des renseignements ou des biens classifiés ou désignés;
- Vous traitez sur SIGNET D des renseignements classifiés ou désignés à un niveau supérieur à Protégé A.

Les commissionnaires sont autorisés à effectuer des vérifications périodiques de sécurité. S'ils remarquent que des classeurs ne sont pas verrouillés ou que des documents de nature délicate sont laissés sans protection adéquate, ou encore que des cadenas ou des clés destinés à des coffres de sécurité sont laissés sur des bureaux sans surveillance, ils sont tenus d'émettre des avis de manquement à la sécurité, et ces manquements sont signalés à ISR.

Lorsqu'un commissionnaire trouve du matériel non protégé, ce matériel peut être saisi et détenu par ISRG. Il doit être réclamé immédiatement par l'intéressé. Si vous vous trouvez dans cette situation, vous devrez apporter l'exemplaire blanc signé de l'avis de manquement à ISRG, lorsque vous récupérez l'information visée par l'infraction.

Voici quelques conseils pour assurer la préservation du matériel de nature délicate :

- Videz toujours le dessus de votre bureau à la fin de la journée; durant la journée, posez le matériel de nature délicate sur votre bureau seulement, et non sur des classeurs, sur le bord des fenêtres ou dans des tiroirs;
- À la fin de la journée, inspectez votre bureau;
- Demandez à quelqu'un d'autre d'inspecter votre bureau;
- Présumez toujours que vous ne retournerez pas à votre bureau lorsque vous partez en réunion; rangez donc tout le matériel de nature délicate dans votre classeur;
- Laissez sur votre bureau une carte d'absence;
- Fermez toujours votre bureau à clé lorsque vous quittez pour la journée ou pour une réunion.

QUELS SONT LES SANCTIONS ET LES RECOURS POSSIBLES ?

Le sous-ministre a le droit d'appliquer des sanctions administratives ou disciplinaires à la suite d'infractions ou de manquements lorsqu'il y a eu manifestement faute professionnelle ou négligence. Les sanctions, selon les circonstances et les antécédents de l'employé, peuvent prendre les formes suivantes :

- une réprimande orale ou écrite;
- la révocation ou l'abaissement de l'autorisation de sécurité ou de la cote de fiabilité;
- la suspension sans traitement;
- le congédiement;
- des poursuites pénales.

QUE SIGNIFIE ‹SÉCURITÉ INFORMATIQUE›

On doit porter une attention spéciale à la sécurité des ordinateurs, du matériel de télécommunications et des systèmes connexes pour deux raisons — la nécessité de protéger les renseignements de nature délicate et notre dépendance à l'égard de ces technologies. La sécurité de la technologie de l'information (TI) vise à garantir :

- la confidentialité des données stockées, traitées ou transmises;
- l'intégrité de l'information et des procédés associés;
- la disponibilité des systèmes et des services d'information.
- l'utilisation acceptable des réseaux électroniques du gouvernement.

La sécurité de la TI vise également le matériel informatique, les logiciels, les réseaux, le matériel de télécommunications et tout autre matériel interconnecté, ainsi que les endroits où se trouve tout ce matériel.

QUELS SONT LES RÉSEAUX MINISTÉRIELS ?

Les systèmes que nous utilisons pour traiter l'information couvrent plusieurs réseaux ministériels, soit :

SIGNET-D
SIGNET-D (Réseau mondial intégré de communications protégées - Désigné) est le principal réseau ministériel utilisé à l'Administration centrale et dans les missions. Il sert à traiter des renseignements non classifiés et des renseignements dont la désignation n'est pas supérieure à PROTÉGÉ A. Tous les employés ont accès à ce système, y compris les employés recrutés sur place. Dans certaines petites missions, un administrateur de système recruté sur place est responsable du système SIGNET-D.

SIGNET-C1, C2 et C4 (remplace le réseau COSICS)
Le système SIGNET-C (C pour classifié) est distinct et différent de SIGNET-D. Tous les employés ayant une autorisation de sécurité allant jusqu'à SECRET-II qui doivent traiter de l'information dont la classification n'est pas supérieure à SECRET s'en servent. Comme on utilise le système SIGNET-C pour les données d'une nature plus délicate, il comporte des dispositifs de sécurité supplémentaires comme :

- un disque dur amovible qu'on peut ranger lorsque les lieux sont laissés sans surveillance;
- un dispositif de cryptage approuvé;
- dans les missions, un système TEMPEST.

IMPORTANT
Souvenez-vous qu'aucun mode électronique de traitement, de stockage, de transmission ou de communication de renseignements n'est sûr, sauf si on utilise du matériel et (ou) des systèmes approuvés conformément aux normes de sécurité établies.

Conseils pour l'utilisation des réseaux

- ☐ Joignez une étiquette de classification ou de désignation à tous les messages imprimés, stockés ou transmis.
- ☐ Effectuez une fermeture de session sur votre poste de travail (SIGNET-D et -C) lorsque vous le laissez sans surveillance.
- ☐ Utilisez des logiciels approuvés sur les serveurs et les postes de travail.
- ☐ N'installez pas de modem dans votre ordinateur et n'établissez pas de connexions avec d'autres ordinateurs ou réseaux, sauf si votre administrateur de système vous y a autorisé.

POURQUOI UTILISER UN MOT DE PASSE ?

Votre mot de passe est la clé pour ouvrir votre compte d'utilisateur. Si vous en avez un, le système vous donnera accès au réseau.

CONSEIL : Lorsque vous vous absentez un certain temps, utilisez la fonction de réponse automatique qui enverra un message prédéfini (p. ex., Je serai absent du 15 au 25 septembre. En cas d'urgence, contactez Sam au 991-1234).

COMMENT DOIS-JE UTILISER LES DISQUETTES ?

Enregistrez vos fichiers de données sur des disquettes approuvées à code de couleur, et apposez sur chacune une étiquette portant la classification ou la désignation appropriée. Les codes de couleur pour les disquettes sont les suivants :

Codes de couleur des disquettes

COULEUR	SYSTÈME À UTILISER	CLASSIFICATION OU DÉSIGNATION LA PLUS ÉLEVÉE
Jaune	Les ordinateurs spécialisés	Très secret
Rouge	SIGNET-C	Secret, Confidentiel, Proteégé B and C
Toutes les autres couleurs	SIGNET-D	Protégé A et Non classifié

Même si la couleur de la disquette indique en principe le niveau de sécurité des renseignements, le niveau de classification LE PLUS ÉLEVÉ devrait également être estampillé sur la disquette.

COMMENT PROTÉGER MON SYSTÈME CONTRE LES VIRUS ?

Pour protéger nos systèmes, un programme de détection de virus a été intégré au réseau, et une vérification est effectuée chaque fois qu'un ordinateur du réseau est mis en marche. En suivant les étapes énoncées ci-dessous, vous pouvez protéger votre ordinateur contre la contamination :

- traitez toutes les disquettes provenant d'autres sources (données par un collègue ou prises dans un paquet scellé) avec prudence et vérifiez-les avant de les utiliser;
- ne laissez pas de disquette dans l'unité de lecture lorsque vous lancez votre système;
- demandez à l'administrateur de système de vous remettre une copie du programme de détection de virus pour l'installer dans votre ordinateur à la maison;
- effectuez une vérification des programmes que vous téléchargez à partir de babillards d'Internet ou qui sont joints aux messages transmis par courrier électronique.

IMPORTANT :
Si vous détectez un virus ou en soupçonnez la présence, communiquez immédiatement avec l'administrateur de système.

UTILISATION D'INTERNET

Internet reste une nouvelle technologie, et son emploi soulève bien des questions qui ne sont pas encore résolues. Le Ministère a publié une série de lignes directrices à suivre lorsque vous utilisez Internet. Vous les trouverez sur l'Intranet du Ministère.

Vous pouvez utiliser Internet dans le cadre des activités reliées à vos fonctions et pour votre perfectionnement professionnel durant les heures de travail. Vous pouvez également naviguer sur Internet pour vos besoins personnels en dehors de vos heures de travail (durant les pauses, à midi, après le travail). Vous pouvez vous brancher sur des sites qui présentent un intérêt pour vous, obtenir des informations sur les avantages sociaux et chercher des sources d'information.

À faire...

- ❒ Assurez-vous que vos propos ne sont pas considérés par erreur comme une politique ou un avis du Ministère;
- ❒ N'oubliez pas que chaque visite sur un site provoque la création d'un témoin qui peut permettre de remonter jusqu'à vous à des fins de marketing et de facturation;
- ❒ N'oubliez pas non plus que le MAECI surveille le trafic sur Internet et sur le courrier électronique en vue de protéger sa réputation et d'éviter les abus;
- ❒ Respectez les lois sur la propriété intellectuelle (données, information, images et logiciels), y compris les lois sur le droit d'auteur. Si vous êtes dans l'incertitude sur quelque sujet que ce soit, appelez l'InfoCentre (944-1776);
- ❒ Protégez la sécurité et l'intégrité de SIGNET-D en vous assurant qu'il n'y a aucun virus dans les documents que vous téléchargez;
- ❒ Utilisez seulement des logiciels commerciaux approuvés pour Internet.

À ne pas faire...

- ❒ Utiliser Internet pour en tirer un avantage financier personnel
- ❒ Utiliser Internet à des fins commerciales (par exemple, la distribution de matériel de publicité non sollicité)
- ❒ Utiliser Internet à des fins illégales ou malveillantes
- ❒ Recevoir du courrier électronique de serveurs de listes sans lien avec le travail
- ❒ Visiter des sites Internet qui contiennent du matériel obscène, haineux ou répréhensible
- ❒ Faire des déclarations trompeuses en votre nom ou au nom du Ministère
- ❒ Employer des termes violents ou vulgaires dans vos messages
- ❒ Divulguer des mots de passe du système ou du réseau
- ❒ Télécharger des informations ou des logiciels de nature commerciale protégés par un droit d'auteur

- ❒ Participer à des activités qui peuvent engorger ou perturber les réseaux ou les systèmes (les chaînes de lettres, par exemple)
- ❒ Accéder sans autorisation à un ordinateur ou un système, au Ministère ou ailleurs
- ❒ Établir des mots de passe collectifs (par exemple, des mots de passe pour les RL) afin d'accéder aux installations ou aux systèmes

QU'EST-CE QU'UNE VÉRIFICATION DE SÉCURITÉ INFORMATIQUE?

ISC procède à des vérifications continues, automatiques et aléatoires de la sécurité sur SIGNET (D et C) et sur d'autres systèmes ministériels. Ces vérifications servent à déceler les manquements et infractions à la sécurité. Dans le cadre du programme sur les infractions de sécurité, les infractions donnent lieu à la délivrance d'un avis de manquement à la sécurité à l'utilisateur identifié. Pour plus d'informations, reportez-vous à la section sur les infractions et les manquements à la sécurité et les sanctions connexes.

SIGLES

AIPRP	Loi sur l'accès à l'information et Loi sur la protection des renseignements personnels
BCM	Service des relations avec les médias
CFP	Commission de la fonction publique
CAC	Clé d'activation cryptographique
CDM	Chef de mission
CPP	Groupe de la planification des politiques
DCP	Bureau du coordonnateur de l'accès à l'information et de la protection de la vie privée
EHS	Évaluation des habilitations de sécurité
GRC	Gendarmerie royale du Canada
ISC	Direction de la sécurité ministérielle
ISD	Direction générale de la sécurité et du renseignement
ISDT	Section du personnel et de l'éducation en matière de sécurité
ISR	Responsable régional de la sécurité
ISRG	Administration centrale, Sécurité
ISSG	Direction des opérations de sécurité
LBP	Édifice Lester B. Pearson
MAECI	Ministère des Affaires étrangères et du Commerce international
MIS	Manuel des instructions de sécurité
MITNET	Réseau de télécommunications internationales mutiutilisateurs
RCN	Région de la capitale nationale
RL	Réseau local
SBA	Direction des services administratifs
SBAD	Gestion des registres d'inventaire
SBAM	Administration centrale, Soutien matériel
SBRP	Politique financière ministérielle, formation et rapports
SCRS	Service canadien du renseignement de sécurité
SERV	Centre de services à l'édifice Lester B. Pearson
SIGNET-C	Réseau mondial intégré de communications - Désigné - Protégé A, B, C et Classifié jusqu'à SECRET
SIGNET-D	Réseau mondial intégré de communications protégées - Non classifié - Désigné et Protégé A
SXT	Direction des opérations
TI	Technologie de l'information
VAF	Vérification approfondie de la fiabilité
VBF	Vérification de base de la fiabilité

GLOSSAIRE

Accès sélectif

Limiter l'accès à certains endroits aux personnes qui doivent y travailler.

Bien de nature délicate

Article, autre que les renseignements, ayant été recensé comme important pour les opérations en vertu de sa fonction ou comme précieux et qui justifie donc d'être placé en lieu sûr (comme les espèces et autres instruments négociables) ou système informatisé qui exige d'être protégé pour assurer l'intégrité et la disponibilité des renseignements qu'il contient.

Biens

Matériel et articles de technologie de l'information précieux, importants, ou tentants. Ils peuvent inclure entre autres :

- les passeports vierges, les étiquettes, les bandes d'indexage;
- les formulaires contrôlés de l'Immigration («Formulaires-clés») comme les visas, permis de travail, permis de séjour pour étudiants, bons de transport, sceaux;
- les timbres humides ou secs, comme les timbres du Ministère ou de la mission, les sceaux secs pour passeports;
- les unités de disques durs amovibles;
- les clés de la mission;
- les clés des téléphones STU-III et des télécopieurs.

Confidentiel

Classification accordée aux renseignements dont une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice à l'intérêt national.

Connaissance sélective

Limiter la diffusion de renseignements aux personnes qui ont besoin de ces renseignements pour leur travail.

Contenant de sécurité approuvé

Contenant conforme à la description donnée dans le Guide de l'équipement de sécurité (DSS/GS20), testé par les douanes et recommandé et approuvé par la GRC.

Endroit contrôlé

Comprend la zone des opérations, la zone de sécurité et de la zone de haute sécurité auxquelles l'accès est réservé aux visiteurs escortés et au personnel autorisé.

Enveloppe

Dossier, pochette ou emballage utilisé pour y glisser des renseignements ou des biens de nature délicate.

Étiqueté

Étiquette indiquant le nom et l'adresse de l'expéditeur ou du destinataire prévu, apposée sur la sacoche de sécurité lorsque celle-ci est utilisée pour le transport de renseignements ou de biens de nature délicate.

EXT-34

Bordereau de transmission utilisé lorsqu'une signature est requise pour accuser réception du document ou quand l'expéditeur veut garder une preuve indiquant que le document en question a été expédié.

EXT -106

Étiquette gommée rouge utilisée sur les enveloppes pour indiquer la cote de sécurité ou de classification et l'adresse du destinataire.

MAECI

Ministère des Affaires étrangères et du Commerce international.

NON CLASSIFIÉ

Renseignement de nature non délicate ne nécessitant aucune des mesures de protection associées aux renseignements désignés ou classifiés.

PROTÉGÉ

Mention utilisée pour décrire les renseignements de nature délicate dont la divulgation risquerait vraisemblablement de causer un préjudice à des intérêts autre que l'intérêt national, et dont le Ministère est responsable. Il existe trois niveaux : A, B ou C, selon la gravité du préjudice que peut entraîner la divulgation des renseignements en question.

PROTÉGÉ «A»

Mention s'appliquant aux renseignements de nature peu délicate, dont une atteinte à l'intégrité risquerait vraisemblablement causer des préjudices (p. ex. : numéros d'assurance sociale, contrats).

PROTÉGÉ «B»

Mention s'appliquant aux renseignements de nature particulièrement délicate, autre que d'intérêt national, dont une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice grave (p. ex. : dossiers médicaux, rapports de police, dossiers financiers, évaluations personnelles, contrats de nature délicate, indications d'opinions politiques, d'associations ou de styles de vie, et toutes informations obtenues.«à titre confidentiel»).

PROTÉGÉ «C»

Mention s'appliquant aux renseignements de nature extrêmement délicate, autre que d'intérêt national, dont une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice extrêmement grave (p. ex., renseignements pouvant mettre la vie en danger, renseignements criminels graves, et renseignements socio-économiques graves concernant une région, une période ou des intérêts particuliers).

PROTÉGÉ (délicat)

Mention anciennement utilisée au MAECI pour désigner à la fois des renseignements classifiés PROTÉGÉ «B» et PROTÉGÉ «C». Voir le Guide de classification et désignation MAECI 13, Supplément I, pour la procédure.

Renseignement classifié

Renseignement se rapportant à la défense et au maintien de la stabilité sociale, politique et économique du Canada, dit normalement d'intérêt national.

Renseignement de nature délicate

Renseignement classifié ou désigné exigeant une protection ou un traitement spécial.

Renseignement désigné

Renseignement non lié à l'intérêt national qui pourrait faire l'objet d'une exception ou d'une exemption en vertu de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels.

Sacoche de sécurité

Porte-documents conforme à la description donnée dans le Guide de l'équipement de sécurité DSS/GS 20, testé et approuvé pour le transport de renseignements et de biens de nature délicate. Fourni aux employés ministériels par la ISDF.

SECRET

Classification accordée aux renseignements dont une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice sérieux à l'intérêt national.

Service exclusif de courrier ou de messagerie

Service assuré par : a) du personnel nommé par les autorités ministérielles pour la transmission courante de renseignements et de biens de nature délicate ou b) une personne approuvée au cas par cas par un employé ministériel pour la transmission de renseignements et de biens de nature délicate.

Service de messagerie fiable

Service de courrier ou de messageries dont les services de distribution ont éprouvé la fiabilité avec d'autres clients, le Bureau d'éthique commerciale, ou la police et qui fournit la preuve de l'envoi ainsi que, sur demande, un bordereau de transit et de livraison.

Service de livraison par porteur

Méthode de livraison du courrier où celui-ci est numéroté et enregistré par l'expéditeur afin de permettre de le retracer et livré par de employés ministériels autorisés de la direction du courrier au sein du MAECI.

EMR (TRA)

Évaluation de la menace et des risques.

Transmettre

Faire transférer des renseignements et des biens d'une personne à une autre ou d'un endroit à un autre par une personne n'ayant pas besoin de ces renseignements ou de ces biens pour son travail.

Transmission

Communication de renseignements par diverses méthodes, p. ex. par valise diplomatique, par messager, par courrier postal, par porteur, ou par voie électronique.

Transporter

Faire transférer des renseignements ou des biens de nature délicate d'une zone à accès réglementé par une personnes sélectionnée ou ayant une cote de sécurité appropriée, qui a besoin de connaître ces renseignements ou d'avoir accès à ces biens pour son travail à une autre personne qui a besoin de ces renseignements ou de ces biens pour son travail.

TRÈS SECRET

Classification de l'information accordée aux renseignements dont une atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice exceptionnellement grave à l'intérêt national.

Utilisateur autorisé

Personne ayant accès aux renseignements qui a une cote de sécurité adéquate ou une cote de fiabilité approfondie et qui satisfait au principe de connaissance sélective.

Zone de haute sécurité

Zone dont l'accès est contrôlé à l'entrée et réservé au personnel autorisé, au personnel sélectionné ainsi qu'aux visiteurs autorisés et dûment escortés, et qui est seulement accessible à partir de la zone de sécurité. La zone de haute sécurité sera séparée de la zone de sécurité par un périmètre construit selon les spécifications recommandée dans l'évaluation de la menace et des risques.

Zone de sécurité

Endroit à accès réglementé, réservé au personnel autorisé et aux visiteurs dûment autorisés et escortés, et seulement accessible par la zone des opérations. La zone de sécurité doit être séparée de la zone des opérations par un périmètre de sécurité.

Zone des opérations

Zone à accès contrôlé, réservée au personnel qui travaille dans cette zone et aux visiteurs dûment escortés. Normalement accessible à partir de la Réception.

TRANSMISSION DE RENSEIGNEMENTS ET

Transmission : Envoi de renseignements ou de biens de nature délicate d'une personne à une autre ou d'un lieu à un autre par une personne dont les fonctions n'exigent pas qu'elle prenne connaissance des renseignements ou ait accès aux biens en question.

MOUVEMENT		CLASSIFICATION OU DÉSIGNATION DES RENSEIGNEMENTS
À L'INTÉRIEUR DE L'ÉDIFICE L.B. PEARSON		PROTÉGÉ A PROTÉGÉ B CONFIDENTIEL SECRET
		PROTÉGÉ C
D'UNE ZONE DU MAECI À L'ACCÈS CONTRÔLÉ[1] À UNE ZONE À ACCÈS CONTRÔLÉ[1] AU CANADA (par ex., Tours Vanier, entre les ministères; aux bureau de sociétés ayant un certificat de sécurité)	SERVICES DU MAECI	PROTÉGÉ A PROTÉGÉ B
		CONFIDENTIEL SECRET
		PROTÉGÉ C
	SERVICES EXTERNES	PROTÉGÉ A PROTÉGÉ B CONFIDENTIEL SECRET
		PROTÉGÉ C
DU MAECI À DES DESTINATIONS À L'EXTÉRIEUR DU CANADA (AUTRES QUE LES MISSIONS)		PROTÉGÉ A PROTÉGÉ B
DE LA CENTRALE DU MAECI À DES MISSIONS CANADIENNES OU ENTRE DES MISSIONS CANADIENNES		PROTÉGÉ A
		PROTÉGÉ B CONFIDENTIEL
		PROTÉGÉ C SECRET

Notes:

1. Zone contrôlée : combinaison de la zone de travail, de la zone de sécurité et de la zone à haute sécurité, auxquelles l'accès est restreint.
2. Adresse : adresser normalement au service responsable; mais lorsqu'il faut restreindre l'accès, ajouter «...À être ouvert seulement par...(nom ou poste)».
3. Les demandes de transmission par méthode spéciale doivent être accompagnées d'un formulaire EXT 1223 (Autorisation d'utiliser un service de messagerie privé).

Attention : Pour les procédures de manutention des documents du Cabinet, des renseignements ou des biens Très secret ou de l'OTAN, consulter le chapitre 2 du *Manuel des instructions de sécurité* ou contacter le Service de distribution du MAECI (SBG).

ET DE BIENS DE NATURE DÉLICATE

PRÉPARATION, PAR L'UTILISATEUR, DES RENSEIGNEMENTS OU DES BIENS DÉSIGNÉS OU CLASSIFIÉS	MÉTHODE DE TRASMISSION PAR LES SERVICES DU COURRIER
UNE ENVELOPPE ADRESSÉE[1] ET SCELLÉE AVEC L'AUTO-COLLANT EXT 106. (PEUT ÊTRE UNE ENVELOPPE À FICELLE)	SERVICE DU COURRIER OU DE MESSAGERIE DU MAECI
DEUX ENVELOPPES ADRESSÉES[3]. ENVELOPPE INTÉRIEURE GOMMÉE ET SCELLÉE AVEC L'AUTO-COLLANT EXT 106. ENVELOPPE EXTÉRIEURE SANS MENTION DE LA COTE DE SÉCURITÉ. (PEUT ÊTRE UNE ENVELOPPE À FICELLE)	
CHAQUE DOCUMENT DANS UNE ENVELOPPE GOMMÉE ADRESSÉE[2] (INSCRIRE ‹PAR PORTEUR› AU BESOIN) AUCUNE MENTION DE LA COTE DE SÉCURITÉ	SERVICES DE COURRIER, DE MESSAGERIE OU DE LIVRAISON PAR PORTEUR DU MAECI
CHAQUE DOCUMENT DANS UNE ENVELOPPE GOMMÉE ADRESSÉE[2] (INSCRIRE ‹PAR PORTEUR› AU BESOIN) AUCUNE MENTION DE LA COTE DE SÉCURITÉ	
DEUX ENVELOPPES GOMMÉES ADRESSÉES[3]. ENVELOPPE INTÉRIEURE AVEC MENTION DE LA COTE DE SÉCURITÉ. ENVELOPPE EXTÉRIEURE SANS MENTION DE LA COTE DE SÉCURITÉ. (INSCRIRE ‹PAR PORTEUR› AU BESOIN)	
UNE ENVELOPPE GOMMÉE ADRESSÉE[2] SANS MENTION DE LA COTE DE SÉCURITÉ	POSTES CANADA 1ÈRE CLASSE OU SERVICE DE MESSAGERIE[4] FIABLE
DEUX ENVELOPPES GOMMÉES ADRESSÉES[3]. ENVELOPPE INTÉRIEURE AVEC MENTION DE LA COTE DE SÉCURITÉ, JOINDRE UN BORDEREAU DE TRANSMISSION (EXT 34) COMPLÉTÉ. ENVELOPPE EXTÉRIEURE SANS MENTION DE LA COTE DE SÉCURITÉ	POSTES CANADA COURRIER RECOMMANDÉ OU SERVICE DE MESSAGERIE[4] FIABLE
UNE ENVELOPPE GOMMÉE ADRESSÉE[2] AVEC MENTION DE LA COTE DE SÉCURITÉ	POSTES CANADA OU COURRIER 1ÈRE CLASSE ÉQUIVALENT À L'ÉTRANGER
UNE ENVELOPPE GOMMÉE ADRESSÉE[2] SANS MENTION DE LA COTE DE SÉCURITÉ	COURRIER DIPLOMATIQUE PAR AVION
UNE ENVELOPPE GOMMÉE ADRESSÉE[2] AVEC MENTION DE LA COTE DE SÉCURITÉ	SAC DU COURRIER DIPLOMATIQUE DU MAECI
DEUX ENVELOPPES. ENVELOPPE INTÉRIEURE GOMMÉE ADRESSÉE[2], AVEC MENTION DE LA COTE DE SÉCURITÉ ET RUBAN INDÉCACHETABLE, JOINDRE UN BORDEREAU DE TRANSMISSION (EXT 34) COMPLÉTÉ. ENVELOPPE EXTÉRIEURE À FICELLE ADRESSÉE2 AU Service de distribution du MAECI, SCELLER AVEC L'AUTO-COLLANT EXT 106	

TRANSPORT DE RENSEIGNEMENTS

Transport : Envoi de renseignements ou de biens de nature délicate, à partir d'une zone à accès contrôlé, entre personnes ayant fait l'objet d'une enquête de sécurité ou ayant une autorisation de sécurité, et dont les fonctions exigent qu'elles prennent connaissance des renseignements ou aient accès aux biens en question.

Notes:
1. Zone contrôlée : combinaison de la zone de travail, de la zone de sécurité et de la zone à haute sécurité, auxquelles l'accès est restreint.
2. Adresse : adresser normalement au service responsable; mais lorsqu'il faut restreindre l'accès, ajouter «...À être ouvert seulement par...(nom ou poste)».
3. Sur l'étiquette, inscrire l'adresse complète de destination ou de retour et le numéro de téléphone du porteur.
4. Contacter la section des services administratifs (ISDF) pour des valises sécuritaires.
Attention : Chaque fois que des frontières internationales sont traversées, l'utilisation de la valise diplomatique du MAECI est recommandée. Pour les procédures de manutention des documents du Cabinet, des renseignements ou des biens Très Secret ou de l'OTAN, consulter le chapitre 2 du *Manuel des instructions de sécurité* ou contacter le Service de distribution du MAECI (SBG).

DESTINATION	
DANS L'ÉDIFICE L.B. PEARSON, À L'INTÉRIEUR D'UNE ZONE À ACCÈS CONTRÔLÉ[1] (À l'intérieur de toutes les tours et entre les tours A, B et C lorsqu'on utilise les passages de raccordement entre tours)	
DANS L'ÉDIFICE L.B. PEARSON, À L'EXTÉRIEUR D'UNE ZONE À ACCÈS CONTRÔLÉ[1] (Lorsqu'on traverse les zones publiques, les halls d'entrée, les corridors du sous-sol ou le garage)	
DE LA CENTRALE DU MAECI À TOUTE DESTINATION AU CANADA (Par ex., Place Vanier, l'AC de TPSGC., Bureau du Conseil privé et autres ministères fédéraux. Les documents doivent rester en tout temps sous le contôle du porteur)	
D'UNE MISSION DIPLOMATIQUE OU CONSULAIRE CANADIENNE À UNE DESTINATION DANS LE PAYS HÔTE	
D'UNE MISSION DIPLOMATIQUE OU CONSULAIRE À UNE DESTINATION À L'EXTÉRIEUR DU PAYS HÔTE	

ET DE BIENS DE NATURE DÉLICATE

DÉSIGNATION OU CLASSIFICATION DES RENSEIGNEMENTS	MÉTHODES APPROUVÉES POUR LES ENVELOPPES ET LES ADRESSES
PROTÉGÉ A PROTÉGÉ B CONFIDENTIEL	ENVELOPPE NON REQUISE (TRANSPORTER DISCRÈTEMENT)
PROTÉGÉ C SECRET	UNE ENVELOPPE SANS MENTION DE LA COTE DE SÉCURITÉ (PEUT ÊTRE UNE ENVELOPPE À FICELLE)
PROTÉGÉ A PROTÉGÉ B PROTÉGÉ C CONFIDENTIEL SECRET	UNE ENVELOPPE ADRESSÉE[1] SANS MENTION DE LA COTE DE SÉCURITÉ (PEUT ÊTRE UNE ENVELOPPE À FICELLE)
PROTÉGÉ A PROTÉGÉ B	UNE ENVELOPPE ADRESSÉE[1] SANS MENTION DE LA COTE DE SÉCURITÉ (PEUT ÊTRE UNE ENVELOPPE À FICELLE)
CONFIDENTIEL SECRET	UNE ENVELOPPE GOMMÉE ADRESSÉE[1] SANS MENTION DE LA COTE DE SÉCURITÉ
PROTÉGÉ C	UNE ENVELOPPE GOMMÉE ADRESSÉE[1] PORTANT LA MENTION DE LA COTE DE SÉCURITÉ ET MISE DANS UN PORTE-DOCUMENTS VÉROUILLÉ ET ÉTIQUETÉ[1]
PROTÉGÉ A PROTÉGÉ B CONFIDENTIEL	UNE ENVELOPPE GOMMÉE ADRESSÉE[1] OU DOCUMENTS MIS DANS UNE VALISE SÉURITAIRE[4] VERROUILLÉE ET ÉTIQUETÉE[1]
PROTÉGÉ C SECRET	DEUX ENVELOPPES GOMMÉES ADRESSÉES[1], AVEC MENTION DE LA COTE DE SÉCURITÉ SUR L'ENVELOPPE INTÉRIEURE SEULEMENT OU DANS UNE ENVELOPPE GOMMÉE ADRESSÉE[1] PORTANT LA MENTION DE LA COTE DE SÉCURITÉ ET MISE DANS UNE VALISE SÉCURITAIRE[4] VERROUILLÉE ET ÉTIQUETÉE[1]
PROTÉGÉ A PROTÉGÉ B PROTÉGÉ C CONFIDENTIEL SECRET	VOIR LES INSTRUCTIONS POUR LA TRANSMISSION ET TRANSMETTRE PAR LA VALISE DIPLOMATIQUE OU CONTACTER LE SERVICE DE DISTRIBUTION DU MAECI POUR UN SERVICE DE MESSAGER SPÉCIAL

SECURITY AND SAFETY *Practices*

in Foreign Affairs and International Trade Canada

IMPORTANT TELEPHONE NUMBERS

IN CASE OF EMERGENCY (Control Centre)	992-1150
Need a new key, combination padlock or new padlock?	992-6678 (ISRG Lockshop)
Need information on disposing of sensitive information?	992-5452 (ISRG Lockshop)
Need an ID Card/building pass or temporary pass?	(ISRG ID Section) 996-8457(SERV) 992-6691(BG-180)
Locked out of your office?	992-6678 (ISRG Lockshop)
Lost something?	944-0019 (ISRG)
Want to know about courses, seminars, briefings, or job aids on security?	992-6704 (ISDT)

September 1998

Table of Contents

About This Document

This handbook is to assist you in performing your security responsibilities as an employee of the Department of Foreign Affairs and International Trade (DFAIT).

From the marking, handling, storage, transmission and proper destruction of sensitive information to the use of secure equipment and access to restricted zones, security will be an important element of your day-to-day decisions. Your security responsibilities start the moment you arrive at work and continue even after your termination of employment.

Use the handbook as a reference document.

Some aspects of both the physical security and the emergency procedures provisions described in this handbook apply specifically to the Lester B. Pearson (LBP) Building in Ottawa. If you are working in other buildings in Ottawa or at locations elsewhere in Canada, including conference sites, you should be aware of the prevailing local security and emergency arrangements. Some of the information can also apply to missions abroad.

Since most of the information contained in this hanbook pertains to Headquarters (the LBP Building), it is not intended to be a substitute for the more comprehensive security policy and instructions established by the Department. You are encouraged to make use of the complete set of policies, procedures, advice and guidance available to you. For more information, consult the Manual of Security Instructions (MSI), the appropriate Section in the Security and Intelligence Bureau (ISD), or the Security Operations Section (ISRG).

If the Handbook doesn't answer all of your questions, ISDT offers some courses and briefings that are scheduled on an as-required basis to people at the division, branch or bureau level. Contact the Security Education and Awareness Program (ISDT) at 992-6704 for its Calendar of Courses which describes available security briefing sessions.

INTRODUCTION

The Department of Foreign Affairs and International Trade (DFAIT or Department) is quite unique when compared to other Canadian government departments. Both the environment in which the Department operates and the departmental mandate have created this uniqueness.

Each day, the Department handles a large volume of correspondence and information, much of which is sensitive. It includes information given to us by foreign governments, other departments, businesses and industries, and individuals. It is important that this information be safeguarded.

The Department also possesses valuable assets, owns and leases chanceries or official residences, including staff quarters, vehicles, works of art and office equipment which are worth millions of dollars. Many Missions generate sizeable cash holdings and travel documents such as passports, visa foils and ministerial permits that require protection.

Canada's overseas programs are also at risk. Export programs are a key element of the Canadian economy and the loss of a major export sale or market because of a security breach can have severe consequences on the Canadian economy.

Often difficult to quantify, yet critical to a nation like Canada, are the "intangibles of state". Canada needs to maintain the trust of other states to ensure a free flow of information. Canada also needs to be able to gain access to and influence decision makers. Care therefore needs to be taken to avoid any suggestion that Canada's credibility is at risk from a security perspective.

The Department's concern for the safety of its employees and their dependants, who are living and working abroad in widely varying environments, many of which are demonstrably more dangerous than that prevailing in Ottawa, is one of the principal feature distinguishing the security policy of DFAIT from that of other Canadian departments and agencies which focus mainly on security of information issues.

> *NOTE*: Security procedures may involve some inconvenience, but good common sense and an ounce of prevention are often all that is required to ensure the safeguards of information and assets, and your personal safety.

WHAT SHOULD I DO IN AN EMERGENCY?

ISRG is responsible for developing and implementing all procedures, orders and instructions for any situation that may affect either the safety or protection of personnel or sensitive information and assets in the LBP Building. ISRG is also responsible for employee training and the supervision of any security standing orders during an emergency situation, threats of fire, bomb incidents, demonstrations, or disturbances.

WHAT ARE THE BUILDING EMERGENCY PROCEDURES?

Simple emergency procedures have been developed for the LBP Building and are available in the Manual of Security Instructions and in the booklet entitled "Emergency Procedures, Lester B. Pearson Building". These procedures are designed to provide a prompt, coordinated and effective response to a wide variety of operational emergency situations, including a fire alert, a medical emergency or a significant building emergency.

You should take time to read and consider these procedures.

WHAT IS THE PEARSON BUILDING CONTROL CENTRE?

The Control Centre monitors all of the security and fire alarms in the LBP Building and the Red Emergency Telephone system. The Centre is located on the ground level of Tower B and is operated 24 hours a day by a bilingual staff of trained members of the Canadian Corps of Commissionaires who are familiar with every aspect of the building. The Commissionnaires can communicate throughout the building during both regular work hours and silent hours. The emergency voice communication system is managed from the Centre and has over 100 red emergency telephones installed throughout the building. The Centre also has a complete set of building floor plans and keys.

If the Centre staff receive notification of an emergency, they will contact all required emergency response services including:

- Municipal and Regional Emergency Response Services; and
- Building Emergency Organization.

Who are Floor Fire Emergency Officers?

Each floor has a team of Floor Fire Emergency Officers (FFEO) who are able to provide direction and emergency assistance. A list of emergency personnel assigned to your floor is posted adjacent to the emergency stairwells on your respective floor. You should familiarize yourself with the names, locations and telephone numbers of the Officers on your floor. During an emergency, the Officers may be identified by their distinctive yellow hard hats.

What should I do in an emergency situation?

In the event of a fire, a medical emergency, a bomb threat, crimes, disturbances, intrusions, building or equipment failures or disaster events, use a Red Emergency Telephone direct line to the Control Centre, or telephone the Control Centre at 992-1150, or use a Fire Alarm Pull Station.

What if I am mobility-impaired?

If you have a mobility or sensory impairment, or may be temporarily impaired because of an injury or medical problem, make yourself known to the person or persons who agree to be your personal monitor, the Floor Fire Emergency Officer (FFEO) in your area, and the Control Centre. If you do this, the Control Centre will be able to manage the situation safely. If you do not wish to disclose your condition, you should advise your FFEO that you may require assistance in the event of an emergency evacuation.

What should I do if there is a Fire?

If you discover a fire, see smoke or smell gas:

- activate the nearest fire alarm;
- evacuate immediately using the nearest stairwell; and
- clear the building to a minimum distance of 100 metres (300 feet).

If you hear the alert signal (ringing of the bells at 20 beats per minute):

- listen to instructions over the emergency public address system; and
- prepare to evacuate when ordered to do so.

If you hear the alarm signal (bells ringing at 120 beats per minute):

- listen to and follow instructions given over the emergency public address system;
- when instructed, evacuate immediately using the nearest stairwell and clear the building to a minimum distance of 100 metres;
- do not attempt to remove your vehicle from the parking garage.

Mobility impaired personnel should await instructions and assistance from their FFEOs as they are trained in First Aid, Fire and Emergency Procedures, the use of fire extinguishers, and emergency threat evacuation procedures.

Fire orders are posted in elevator lobbies and other strategic locations such as the entrances to towers. You should read them and familiarize yourself with the fire equipment location and evacuation routes to follow in the event of a fire emergency.

WHAT SHOULD I DO IF THERE IS A BOMB THREAT?

If a bomb threat is received or a suspicious object or package is found, do not handle the item. Contact the Control Centre immediately! It is important for you to report the incident in as much detail as possible so that appropriate decisions on any action can be taken.

For more detailed information, refer to the Emergency Procedures - Employee Handbook and to the RCMP brochure Bomb Threat Telephone Procedures. These publications are available at the entrances to the towers on the ground floor and main (first) floor levels.

WHAT SHOULD I DO IF THERE IS A DEMONSTRATION?

The LBP Building may be subject to demonstrations or occupation through unauthorized or forcible entry. If such a disturbance occurs, observe the following precautions:

- do not personally interfere with or try to stop any form of demonstration;
- do not encourage or argue with participants;
- do not place yourself in a position where you risk being taken hostage;
- do not attempt to secure sensitive material if you are at risk;
- advise and support your co-workers in the avoidance of confrontations; and
- observe the actions and identity of the participants.

WHAT IF SOMETHING IS STOLEN OR LOST?

Protect your personal property by keeping your purse, wallet, money and any items of sentimental value in your possession or secured at all times. Remember, desk drawers are not secure.

Please remember, as well, that it is also your responsibility to safeguard valuable Government property such as calculators, computer equipment (especially laptop/notebook computers), tape recorders, or cameras by placing such items in locked cabinets or rooms when not in use.

If you experience a loss or theft, report it to the ISRG (Security Operations) at 944-0019. If you experience the loss of government property report it to SBAD (Headquarters Inventory Records Management) at 996-6816 and to the SBRP (Corporate Financial Policy, Training and Reporting) at 944-1102.

THE SECURITY OF INFORMATION?

The Government Security Policy establishes a framework of policy guidelines for implementing information security and privacy requirements. This framework requires the Department to properly safeguard personal information and other sensitive data contained in its information systems or used in its programs and services. The policy is based on the principle that safeguards for information and assets should clearly reflect their sensitivity, importance and value—no more and no less.

Your responsibility is to protect the sensitive information and assets that you handle on a day-to-day basis. This means protecting it against unauthorized disclosure, destruction, removal or modification. No one wants to compromise any information that could endanger the national interest or other interests for which Parliament assumes an obligation.

In your day-to-day work, make sure that you can:

- ✔ identify information that is sensitive;
- ✔ choose the appropriate level of sensitivity for information you create, and,
- ✔ mark this information correctly so others see the need for special protection.

You should also be able to:

- ✔ select secure equipment and a secure location to write, discuss and transmit information;
- ✔ store information securely; and
- ✔ destroy the information safely and securely.

WHAT IS SENSITIVE INFORMATION?

Not all information needs to be classified or designated. However, at a minimum, departmental information and assets should receive a level of reasonable care that is consistent with basic administrative practices. Certainly, information should never be classified nor designated to conceal violations of the law, inefficiencies or administrative errors, nor to avoid embarrassment or to restrain competition.

It is true, however, that some information and certain assets are more sensitive or valuable than others 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* you are responsible for identifying the level of sensitivity for the information you create.

The departmental Classification and Designation Guide, available on the DFAIT Intranet, provides appropriate classification guidelines. You may also contact the Corporate Security Division (ISC) for additional information.

There are three levels of information sensitivity: Unclassified, Designated and Classified.

EXAMPLES OF CLASSIFIED INFORMATION

TOP SECRET

- information on potential armed hostilities toward Canada or its allies
- information about methods and successes in national intelligence and counter intelligence services
- reports, the dissemination of which could result in death or torture of an individual whose life is in the national interest

SECRET

- minutes of discussions of Cabinet or Cabinet committees
- reports concerning important international negotiations
- scientific or technical reports relating to national defence or national security

CONFIDENTIAL

- records of discussions of interdepartmental committees
- instructions for the protection of highly classified information
- reports from Missions or from Canada that may be of use to foreign powers or that could cause damage to international relations

EXAMPLES OF DESIGNATED INFORMATION

PROTECTED C

- reports, the dissemination of which could endanger the safety of an individual
- reports containing extremely sensitive commercial information

PROTECTED B

- records of discussions that involve the solicitor-client privilege
- reports on a company's financial status
- completed appraisal report

PROTECTED A

- an exact salary figure of an employee
- a Social Insurance Number

NOTE: Remember to always mark the information you create appropriately.

EXTRACTING CLASSIFIED INFORMATION

Information extracted from material that is already classified or designated is automatically classified/designated to match the original information. For example, if a document is classified as SECRET, a person preparing a covering briefing note simply classifies the briefing note as SECRET.

The Classification and Designation Guide also provides you with information on how to mark the following:

- Bibliographies and sources
- Charts and maps
- Films and negatives
- File folders
- Forms
- NATO documents
- Documents for external use
- Documents with Caveats

AUTOMATIC DECLASSIFICATION OR DOWNGRADING

Information must be classified/designated only for the time it requires protection. Once that time has elapsed, the classification/designation should be removed or downgraded. When you create a document you can specify a date or event after which the document can be automatically declassified/downgraded.

Examples:

1. Confidential (Unclassified after 31 July 1999)
2. Protected A (Unclassified if Annex A removed)

CHANGING A DOCUMENT'S CLASSIFICATION OR DESIGNATION

If you want to change the classification or designation of a document you must:

- be the author or an employee who replaced the author in a position;
- have a clear proprietary responsibility for the information; and
- have a detailed knowledge of, and be familiar with, the sensitivity of the information.

The date, authority, and the new classification/designation should be clearly marked in ink on the document or asset.

You should make every effort to involve the originator of a document before you change its classification or designation, but circumstances do arise (e.g., requests under the *Access to Information or the Privacy Act*) where information may be declassified and released without the involvement or knowledge of the originator.

If a classification or designation is removed or downgraded, this does not mean that it can, or should be, released to the public. Requests for information by the public, the media, industry, etc., should be referred to the Media Relations Office (BCM) or to the Office of the Coordinator for Access to Information and Protection of Privacy Division (JIP).

PERSONNEL SECURITY

WHO CAN HAVE ACCESS TO SENSITIVE INFORMATION?

An important and fundamental principle of good security is the "need to know". This principle involves limiting access to designated or classified information or assets to only those people who must have access to it in order to perform their jobs. No employee is entitled to have knowledge or custody of classified information solely by virtue of a level of security clearance.

You, like other departmental employees had to undergo a security screening process before being appointed to your position.

There are two types of security checks:

- the Basic/Enhanced Reliability Check (B/ERC)
- the Security Clearance Assessment (SCA)

NOTE: To have access to the L.B. Pearson building operation zone, a SECRET clearance is required.

WHAT IS THE BASIC/ENHANCED RELIABILITY CHECK?

This check must be carried out by the hiring manager, staffing officer or administrative officer before a security clearance can be requested and prior to the appointment of an individual. Once you are granted this status you may have access to unclassified and designated information and assets.

These checks include verifying and checking:

- personal and employment data;
- educational and professional qualifications;
- accreditations or certifications;
- references;
- criminal records;
- credit rating; and
- names indices (VETTING).

Once the ERC is completed access is given to designated information (Protected A, B and C).

WHAT IS A SECURITY CLEARANCE ASSESSMENT?

A security clearance assessment is required for anyone who has access to classified information or assets, regardless of the type of assignment. This assessment is completed in addition to the Basic/Enhanced Reliability Check. It may include a check of:

- your character references;
- your personal background which may cover a period of 10 years or more; and
- the Canadian Security Intelligence Service (CSIS) indices;

There are three levels of security clearances, which correspond to the three levels for classified material:

Level I - access to CONFIDENTIAL

Level II - access to SECRET

Level III - access to TOP SECRET

A Level II -SECRET clearance is a mandatory minimum requirement for employment at the Lester B. Pearson building.

A Level III - TOP SECRET clearance is the minimum requirement for members of the rotational foreign service posted abroad.

Points to remember:

✔ A security clearance is required whether you are a full-time, temporary, or contract employee.

✔ The status of your security clearance may be updated as required, and MUST be updated every five years for Level III clearance and every ten years for Level I and II clearances.

- ✔ Your security clearance level is transferable if you move from one position to another position within the Department, if you contract to another Department or are seconded to another Department, or if you move to another Department.

Marriage or Cohabitation

If you have a valid security clearance and plan to marry or cohabit (including a same-sex relationship), complete Form EXT 332 Intent to Marry or Cohabit and submit it to ISDT for security verification. Based on the information you provide on the form, a security assessment will be carried out. This particular assessment is not the same as any of the procedures used to grant a security clearance.

When You Leave the Department

Managers or Staffing Officers are required to complete an Administrative Cancellation of Enhanced Reliability Check/Security Clearance Form - TBS/SCT 330-25 for every employee leaving the Department. This form should be submitted to ISDT at least two weeks prior to the end of employment.

Removal/Revocation of Reliability Status or Security Clearance

As a result of an update or a review based on new adverse information concerning an individual, his/her reliability status or security clearance may be revoked.

The authority to deny, revoke or suspend a security clearance rests with the Deputy Minister and may not be delegated.

The authority to deny, revoke or suspend a reliability status rests with the responsible manager.

In both instances, the individual is informed of his/her rights of review or redress and prohibited from access to sensitive information and assets. When the individual is informed of the reasons for denial, her/she is also advised of the right to redress.

WHAT IS PHYSICAL SECURITY?

Physical security includes all the measures taken to protect sensitive information and assets and to ensure the safety of personnel, including:

- day-to-day monitoring of the flow of people into restricted zones of the Lester B. Pearson Building;
- identification (ID) cards/building passes;
- closed circuit television surveillance of some entry and exit points;
- locker safes and other approved cabinets;
- vaulted registries;
- approved paper shredders;
- alarm systems and associated equipment;
- mail x-ray; and
- intrusion detection and access control systems, and building public, reception, operations, security and high security zones.

WHERE ARE THE RESTRICTED ZONES?

All the premises occupied in part or in whole by the Department are divided into a number of restricted zones. This is to control access, to protect all government assets and to ensure the safety of personnel.

Public Zone:
This zone surrounds or forms part of the facility. Examples in the LBP Building include the cafeteria, the Royal Bank and the lobby.

Reception Zone:
Located at the entrance to the building, this zone is defined by the area where initial contact occurs between the public and the Department. It is further defined as the area where services are provided, where information is exchanged, and where access to restricted zones is controlled. An example of this type of zone in the LBP Building is the Services Centre (SERV).

Operations Zone:
Access to this zone is limited to personnel and to visitors who are escorted by employees with a security clearance. In the LBP Building, this would include all the towers.

Security Zone:
This zone limits access to authorized personnel and visitors who are escorted by employees with a security clearance. These zones are monitored at all times by security staff, other personnel or by electronic means.

High-Security Zone:
Entry points control access to this zone. Access is limited to authorized appropriately-screened personnel and visitors who are escorted by employees with a security clearance. These zones are monitored at all times by security staff, other personnel or by electronic means.

Floor 9 of Tower A:
This is an area where departmental functions are hosted for visitors who have been escorted to and from the floor through Tower A. Visitors are not allowed unescorted access to other floors of Tower A or to any other tower.

HOW DO I ACCESS A RESTRICTED ZONE?

Swipe card entry devices are installed at the entrance of each tower. The following three colours of departmental and temporary building passes allow access to the LBP Building.

Blue Pass:
The Blue pass gives access to the restricted zones 24 hours a day, 7 days a week. This pass also allows you to escort visitors or employees who do not have a building pass to restricted areas of the Department. To get a Blue pass you must have, at a minimum, a Level II (SECRET) security clearance.

Green Pass:
The Green pass gives access to the restricted zones during core hours only - 0700 to 1800 hours, Monday to Friday, except statutory holidays. You cannot escort visitors on the premises with this pass. At a minimum, a Level II (SECRET) security clearance is required to get a Green pass.

Red Pass:
The Red pass is for personnel who do not normally need access to restricted areas and/or who are not security cleared to at least SECRET. With a red pass, you must be escorted in restricted areas.

Temporary Building Passes:
Temporary building passes are only issued if you already have a Blue or Green pass and you forget or misplace it. Your original pass is deactivated when you request a temporary pass and is reinstated when you return the temporary pass.

If you are transferred or your employment is terminated, you must return your pass. If you lose your pass, immediately contact the ISRG Identification Section.

Services Centre (SERV):	996-8457
ID Room (BG-180):	992-6691

Please keep in mind that it is your responsibility to ensure that anyone entering one of the towers behind you is authorized to do so.

How do I get a building pass?

Cards are issued by ISRG at two locations—the Services Centre (SERV) located off the main lobby (8:30 to 11:30 a.m. and 1:00 to 2:30 p.m.) and the ISRG Identification Section which is located in Room BG-180 (7:00 a.m. to 4:00 p.m.).

Visitor Access

Visitors to restricted areas need to be escorted at all times. Violation of this responsibility may result in a security infraction.

It is your responsibility to escort those individuals back to a public area or arrange to have someone else escort them back to a public area. This includes outside participants to a meeting held in the Lester B. Pearson Building.

WHAT ACCESS IS ALLOWED TO RESTRICTED AREAS DURING QUIET HOURS (WEEKDAYS 4:00 P.M. TO 8:00 A.M., WEEKENDS AND HOLIDAYS)?

Even though there is a swipe card system, it is still mandatory to sign in and out of the LBP Building during quiet hours. This record will indicate who and where personnel are located in the building in case of an emergency such as a fire.

WHAT ABOUT THE ALARM SYSTEMS?

Access control doors located at the entrance to the towers in the LBP Building are protected by alarm systems which can be activated during limited access hours. If you want to enter controlled areas during silent hours, coordinate your request with the Commissionaire on duty. If you attempt to enter any other restricted zone during these hours, you may trigger an alarm that will result in a security response.

WHAT ROLE DOES SECURITY HAVE REGARDING PARKING?

Parking permits are issued by the Headquarters Administrative Services Division (SBA) located on the ground level of Tower A in the LBP Building. If you have any questions about these permits, you should contact SBAA (992-2338). ISRG, through a special arrangement with the RCMP, enforces the parking regulations established by the Government Property Traffic Act.

WHAT ARE THE RESPONSIBILITIES OF THE CANADIAN CORPS OF COMMISSIONAIRES?

The Canadian Corps of Commissionaires provides security guard services in the LBP building. They may request the presentation of ID Cards. Commissionaires are responsible for:

- reception and access control;
- monitoring and responding to the building alarm systems;
- conducting security and fire patrols;
- controlling and escorting visitors to an employee's office after contacting that employee; and
- monitoring the movement of material in/out of the LBP Building.

How Do I Handle Sensitive Material?

There are many documents coming in and out of the Department. Some are more sensitive than others. In certain cases, the material must be transported "by hand" to maintain control of the material at all times. In other cases, the material can be transmitted by postal or courier service, provided that the information is properly packaged.

Transmittal of Sensitive Information and Assets

(See appendix A on pages 36 and 37)

Transportation of Sensitive Information and Assets

(See appendix B on pages 38 and 39)

What is a Secure Telephone?

A secure telephone known as a STU-III provides a secure telephone capability for all personnel who have the need to discuss or transmit classified and sensitive information. The STU-III terminal may be used as an ordinary telephone, completely interoperable with the public switched telephone network. It may also be used in a secure mode when the cryptographic module is activated and the terminal is communicating with another STU-III via the public network. STU-IIIs are accountable Controlled Cryptographic Items (CCI). The terminal, on its owns, is UNCLASSIFIED, the Cryptographic Ignition Key (CIK), on its own, is also UNCLASSIFIED. However, upon insertion of the CIK inside the terminal, the item's classification becomes that of its classified Operational Crypto Fill.

The following conditions are possible security compromises and must be reported immediately to ISDF:

- when a STU-III terminal is lost or stolen
- when a CIK is lost or stolen
- when a CIK has been left in the terminal unattended, it is usually considered a security infraction with possible compromise;
- when a STU-III appears to be tampered with.

WHAT IS A SECURE FACSIMILE?

Equipment for the secure facsimile transmission of documents (up to Secret) is available in many offices. Controls are similar to those used for the STU III telephones and if you are authorized to use such equipment, you will be instructed in its use and care.

Never assume that regular telephones, cellular phones, car phones, fax equipment, e-mail or any other electronic means of communication are secure.

Never use such methods of communication to transmit sensitive information.

HOW DO I STORE SENSITIVE MATERIAL?

You are responsible for ensuring that all classified or designated information in your possession is protected at ALL times.

If you are away from your office for an extended period of time, securely lock your doors and windows and store sensitive material in a locked, approved cabinet or safe.

You also need to protect sensitive information during lunch hours, silent hours, weekends and holidays, or during any lengthy absence during working hours (unless the area will be supervised by another security cleared staff member for the entire duration of your absence).

HOW CAN I DISCUSS SENSITIVE INFORMATION?

- Sensitive information should not be discussed in public places nor on open or unsecured telephone lines.
- When you discuss sensitive information with someone, make sure that the person is informed of the information's classification or designation.
- In the case of a lecture or other public event, the audience should be advised of the sensitivity of the information at the beginning and end of the event.
- You may discuss sensitive information using the Secure Telephone (STU III). Consult the *Manual of Security Instructions* for detailed instructions.

WHAT ARE THE MINIMUM STORAGE REQUIREMENTS FOR SENSITIVE MATERIAL?

The minimum requirements for storing sensitive material in Canada are the following:

Top secret:
Must be stored in a high security zone and locked in an approved safe.

Confidential, Secret, Protected A,B,C:
May be stored in an operation zone in an approved security file cabinet with double hasp and approved Sargent & Greenkof (S&G) combination padlock.

WHEN SHOULD A COMBINATION LOCK SETTING BE CHANGED?

Combination settings should be changed:

- when the person knowing the combination is transferred, terminated, or no longer requires access to the information
- when the combination is or may have been compromised
- at least every year

WHAT ABOUT KEYS TO OFFICES?

The Division Secretary or the person responsible for keys in your Section will give you the key to your office. You are responsible for returning that key to the same person when you no longer occupy the office.

If you lock yourself out of your office or forget your key at home, you should ask the Division Secretary or person responsible for keys in your Section to unlock the door. If neither person is available, telephone the ISRG Lockshop at 992-6678 to have the door unlocked. The ISRG Lockshop will do so, but the response time will depend upon the availability of personnel.

- protect your keys at all times
- do not copy keys; spare keys are controlled by Division Secretaries
- new keys may be obtained by the division secretary e-mailing the request to the ISRG Lockshop

Failure to adequately safeguard keys is a SECURITY INFRACTION.

WHAT ARE ABSENT CARDS?

Absent cards are used to prevent classified/designated documents or materials from being delivered and left on desks when employees are absent.

If you know you will be away, get an Absent Card from SBAM and put it on the top of your desk and do not leave any classified/designated documents or materials on your desk.

CAN I REMOVE SENSITIVE MATERIAL TO WORK ON IT AT HOME?

Sometimes you may need to work with classified/designated material during the evenings or on the weekend, but the practice of taking classified/designated information home or any other place is dangerous and is prohibited. Under certain circumstances however, permission may be given in Ottawa by the Director of a Division.

If permission is granted it will be subject to the following conditions:

- you will not be allowed to take TOP SECRET information
- you will be personally responsible for the custody of the material
- you must remain in personal possession of the information at all times.

Equipment and material (including computer equipment and software) cannot be removed from DFAIT premises without a completed GC 205 "Authority for Removal of Material from Premises" form. Likewise, use form GC 205 to remove personal belongings that may appear to be government property.

HOW SHOULD I DISPOSE OF SENSITIVE INFORMATION?

Classified (Confidential and Secret) and Designated (Protected B and C) documents must be disposed of by using the shredders located on all floors of the LBP Building. If you have a large volume of classified waste (for example, if your Division is relocating or wish to dispose of Top Secret documents), call ISRG at 992-6678 to arrange for pick-up or for guidance.

How should I handle Cabinet documents?

Cabinet documents are circulated by hand to Ministers, the Deputy Minister and to departmental employees who have a need to see them. All Cabinet documents "in" and "out" and the name of the officer responsible for the security of the document are recorded in a register in CPP. A bring-forward system is also maintained and officers are sent reminders when the document is nearing its return date.

It is your responsibility to ensure Cabinet documents' safe custody and return. Under no circumstances should you copy or reproduce these documents.

What should I do with sensitive information when I leave?

Regardless of the circumstances under which you leave your employment, it is important to understand and adhere to your security obligations. On departure, you are personally responsible for clearing your filing cabinets and other storage facilities and ensuring that no records, computer diskettes, or other materials are improperly removed or destroyed.

Documents must be disposed of in accordance with the National Archives Policy and the departmental security requirements.

You must also:

- ✔ Return to your supervisor all documents containing classified information, as well as any government assets obtained during your period of service.
- ✔ Return your ID card to the Identification Section in room BG-180 or in SERV, Room D1-425.
- ✔ Complete form TBS-SCT330-25: Administrative Cancellation of ERC/Security Clearance Form

WHAT ARE BREACHES AND VIOLATIONS OF SECURITY?

A security breach is an unauthorized disclosure or access to classified or designated information. It can also be the loss, theft or deliberate damage of designated or classified equipment or materials.

If a security breach occurs, immediately report the incident to your supervisor and to the Departmental Security Officer (ISD). You are cautioned never to delay reporting a suspected breach of security because of embarrassment or to avoid responsibility. Further serious harm may be caused by such a delay.

A security violation is a failure to comply with security policies and procedures that could have led to a security breach, but did not. Such violations could occur if a person:

- failed to classify or designate information according to the Goverment Security Policy;
- classified or designated information in contravention of the Government Security Policy;
- altered, kept, disclosed, or removed classified or designated information or assets without authorization; or
- failed to protect classified or designated information or assets.
- processed classified or designated information above Protected A on SIGNET-D

Commissionaires are authorized to conduct periodic security checks. If they notice unsecure cabinets, sensitive documents left exposed without adequate protection, or combinations or keys for security containers left in open desks, they are required to issue Security Infraction Notices and these violations will also be reported to ISR.

When unsecured material is found, it can be impounded and held by ISRG. This material must be claimed immediately by the person concerned. If you are in this situation, you will need to return the signed white copy of the infraction notice to ISRG when you retrieve the confiscated material.

Here are a few things that you can do to ensure that sensitive material is safeguarded:

- adopt a clean desk policy; during the day, place sensitive material on your desk only, not on cabinets, window sills or in desk drawers;
- at the end of each day do a visual check of your office;
- ask someone to help you do a visual check of your office;
- always assume that when you leave for a meeting you will not be returning, and store all sensitive material in your cabinet;
- leave an Absent Card on your desk; and
- always lock your office when leaving for the day or for a meeting.

WHAT ARE SANCTIONS AND REDRESS?

The Deputy Minister has the right to apply administrative and/or disciplinary sanctions in response to breaches and violations when there is evidence of misconduct or negligence. Sanctions, depending on the circumstances and the record of the employee, may include:

- a verbal or written reprimand;
- revocation or reduction of security clearance or reliability status;
- suspension without pay;
- dismissal; or
- criminal charges.

WHAT DOES "SECURITY OF INFORMATION TECHNOLOGY" MEAN?

The security of computers, telecommunications equipment and related systems requires special consideration for two reasons — the need to protect sensitive information and the extent to which we depend on these technologies. The security aspects of Information Technology (IT) are intended to ensure the:

- confidentiality of information stored, processed or transmitted
- integrity of information and related processes
- availability of information systems and services
- acceptable use of government electronic networks

IT security includes the hardware, software, networks, telecommunications and other equipment that is interconnected, and the facilities in which the equipment is housed.

WHAT ARE DEPARTMENTAL NETWORKS?

The systems we use to process information comprise several departmental networks. They are :

SIGNET-D

The main departmental network used at Headquarters and Missions is SIGNET-D (Secure Integrated Global Network - Designated) network. It is used to ***process unclassified information and information designated up to PROTECTED A***. This system is accessible to all employees including locally-engaged staff abroad. In some small missions the SIGNET-D system is administered by a locally-engaged system administrator.

SIGNET-C1, C2 and C4 (replacing COSICS)

SIGNET-C (C for classified) is distinct and separate from SIGNET-D. This network is available to all employees cleared to level II-SECRET who have a need to know for processing information classified up to SECRET. Because SIGNET-C is used for more sensitive information, it has extra security features such as:

- a removable hard drive that can be stored when unattended
- approved encryption
- at missions, TEMPEST equipment

IMPORTANT
Remember that no means of processing, storing, transmitting or communicating information electronically is secure unless approved equipment and/or systems are used according to the established security standards.

Tips for Network Use

- ❒ include a classification/designation label on all messages that are printed, stored or transmitted
- ❒ log off your workstation (SIGNET-D AND -C) when you leave it unattended
- ❒ use approved software on servers and workstations
- ❒ do not install modems or connections to other computers or networks, unless authorized to do so by your system administrator

WHY USE A PASSWORD?

Your password is the "key" to your user account. If you have a password, the system permits you access.

TIP: When you are absent for a period of time, use the "automatic reply" function which will send a pre-defined message (i.e. absent from 15 to 25 September. If urgent, contact Sam at 991-1234)

How should I use diskettes?

Use the approved colour coded diskettes for your data files and label each disk with the correct classification or designation. The colour codes for diskettes are listed below.

Diskette Colour Codes

COLOUR	SYSTEM TO BE USED	HIGHEST CLASSIFICATION OR DESIGNATION
Yellow	Specially designed computers	Top Secret
Red	SIGNET-C	Secret, Confidential, Protected B and C
All other colours	SIGNET-D	Protected A and Unclassified

Even though the diskette colour "technically" identifies the level of sensitivity of the information it contains, the diskette should also be stamped with the HIGHEST level of classification of the information.

How can I protect my system from viruses?

To protect our systems, a virus detection program is incorporated into the network and a scan is conducted every time a network computer is booted. By following the steps below, you can protect your computer from a virus infection.

- treat all disks from other sources (your co-worker or disks in sealed packages) with caution and scan them before use
- remove disks from your floppy drive when you boot your system
- ask your System Administrator for a copy of the Virus scan program for your computer at home
- scan documents and programs you download from the Internet and Bulletin Boards or that are attached to e-mail messages

IMPORTANT:

If you suspect or detect a virus, immediately contact your System Administrator.

Use of the Internet

The Internet is still a new technology and many questions are still unanswered with respect to its use. The Department has issued a set of guidelines to be followed when using the Internet and these are available on the departmental INTRANET.

You can use the Internet for work-related professional activities and career development during working hours. You can also use the Internet for personal use during your own personal time (breaks, lunch hour, or after work hours). This means you can connect to resources of a personal interest, get information on employee benefits, and search for information sources.

Do

- ❒ make sure that your representation of the Department could not be mistaken as departmental policy or opinion
- ❒ remember that a footprint (a record) is left at each site you visit and this footprint can be traced back to you and used for marketing and billing purposes
- ❒ remember that the Department monitors Internet traffic and e-mail traffic in an effort to protect its reputation and guard against abuse
- ❒ respect the laws relating to intellectual property (data, information, images, information and software), including copyright laws. If you aren't sure about such things, call the InfoCentre (944-1776).
- ❒ protect the safety and integrity of SIGNET-D by checking for viruses on anything you import from the Internet
- ❒ use only approved commercial software programs for Internet use

Do not

- ❒ use for personal gain
- ❒ use for commercial activities (for example, the unsolicited distribution of advertising material)
- ❒ use for unlawful or malicious activities
- ❒ use to receive list-server e-mails that are not work-related
- ❒ visit Internet sites that contain obscene, hateful or other objectionable materials
- ❒ misrepresent yourself or the Department
- ❒ use abusive or objectionable language in your messages
- ❒ share network or system passwords with anyone
- ❒ up or download information or commercial software in violation of copyright
- ❒ involve yourself in activities that can cause congestion or disruption to networks or systems (for example, chain letters)

- ❒ attempt any unauthorized break into any computer or system, whether it is the Department's or another organization
- ❒ establish group passwords (for example, LAN passwords) for facilities or systems access

WHAT ARE IT SECURITY VERIFICATIONS?

A continuous, automated and random program of security verifications on SIGNET (both D and C), and other corporate systems, is conducted by ISC. The purpose of these verifications is aimed at detecting security breaches and violations. As part of the security infraction program, violations result in the issuance of a security violation notice to the identified user. For more information, please refer to the section on Violations, Breaches and Related Sanctions.

ACRONYMS

ATIP	Access to Information and Privacy Acts
BCM	Media Relations Office
BFEO	Building Fire Emergency Officers
BRC	Basic Reliability Check
CPP	Policy Planning Staff
CSIS	Canadian Security Intelligence Service
DCP	Access to Information and Protection of Privacy Division
DFAIT	Department of Foreign Affairs and International Trade
ERC	Enhanced Reliability Check
FFEO	Floor Fire Emergency Officers
HOM	Head of Mission
ISC	Corporate Security Division
ISD	Security and Intelligence Bureau
ISDF	Management Services Unit
ISDT	Personnel Security and Security Education Division
ISR	Physical Security and Personal Safety Division
ISRG	Security Operations Section
IT	Information Technology
LAN	Local Area Network
LBP	Lester B. Pearson Building
MITNET	Multi-User International Telecommunications Network
MSI	Manual of Security Instruction
NCR	National Capital Region
PSC	Public Service Commission
RCMP	Royal Canadian Mounted Police
SBA	Headquarters Administrative Services Division
SBAA	Facilities Management
SBAD	Headquarters Inventory Records Management
SBAM	Headquarters Materiel Support
SBRP	Corporate Financial Policy, Training and Reporting
SCA	Security Clearance Assessment
SERV	Services Centre in Lester B. Pearson Building
SIGNET-C	Secure Integrated Global Network - Classified
SIGNET-D	Secure Integrated Global Network - Designated
SXT	Infrastructure Technology Division

GLOSSARY

Approved Security Container-

a container as described in the Security Equipment Guide (SSB/SG 20) which has been examined in accordance with the custom-test program and recommended and approved by the RCMP.

Assets-

material and information technology articles of value or importance, or desirability. They may include, but are not confined to:
- passport blanks, labels, inserts;
- Immigration controlled forms ("Key Forms") e.g. visas, employment and student authorizations, transportation warrants, seals;
- dry and wet seals, rubber stamps: e.g. departmental and mission seals, passport dry seals;
- computer removable hard drives;
- mission keys;
- STU-III telephone and facsimile keys.

Authorized User-

individuals having access to information who hold the appropriate security clearance or enhanced reliability status and have a need-to-know.

By-Hand Unit-

mail delivery method whereby mail is numbered and registered by the sender to enable tracking and then delivered by authorized departmental personnel employed by the mail division within the DFAIT premises.

Classified Information-

information which concerns the defence and maintenance of the social, political, and economic stability of Canada, normally referred to as "in the national interest".

Confidential-

the classification of information which could reasonably be expected to cause injury to the national interest if compromised.

Controlled Area-

the combination of Operations Zone, Security Zone, and High Security Zone to which access is restricted to properly escorted visitors and authorized personnel.

Designated Information-

information, other than in the national interest, that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act.

DFAIT-

Department of Foreign Affairs and International Trade.

Envelope-

the jacket, wrapper, or cover used to enclose sensitive information and assets.

EXT 106-

red gummed label for use on envelopes to indicate security designation or classification and addressee.

EXT 34-

Transmittal and Receipt Note is used when a signature acknowledging receipt of documents is needed or when the sender wishes to keep a record that the document has been sent.

High Security Zone-

is an area to which access is controlled through an entry point and limited to authorized, appropriately -screened personnel and authorized and properly-escorted visitors and only accessible from the Security Zone. The High Security Zone will be separated from the Security Zone by a perimeter built to specifications recommended in the Threat and Risk Assessment.

Need-to-Access-

limiting access to areas, and assets to those who need to work there.

Need-to-Know-

limiting access to information to those whose duties require such access.

Operations Zone-

is an area where access is controlled and limited to personnel who work there and to properly-escorted visitors. Normally accessible only through the Reception Area.

Proprietary Mail or Messenger Service-

a service provided by : (a) personnel appointed by the departmental authority for the routine transmittal of sensitive information and assets, or (b) an individual endorsed on a case-by-case basis by a departmental employee for the transmittal of sensitive information and assets.

PROTECTED-

a designation used to describe sensitive information the disclosure of which could cause injury to interests other than national interests and for which the department is responsible. Information can be designated at three different levels Protected A, B,or C depending on the gravity of the injury.

PROTECTED A-

a designation applied to low sensitive information, other than in the national interest, that if compromised, could reasonably be expected to cause injury (e.g., Social Insurance Numbers, Contracts).

PROTECTED B-

a designation applied to particularly sensitive information, other than in the national interest, that if compromised, could reasonably be expected to cause serious injury. (e.g., medical records, police reports, financial records, personal assessments, sensitive contracts, indications of political beliefs, associations or lifestyles, and information received "in confidence").

PROTECTED C-

a designation applied to extremely sensitive information, other than in the national interest, that if compromised, could reasonably be expected to cause very serious or grave injury. (e.g., life threatening information, serious criminal intelligence and grave socio-economic information applicable to a geographic area, time frame or interest).

PROTECTED - Sensitive-

a former designation used by DFAIT to describe both PROTECTED B and PROTECTED C information. See the Classification and Designation Guide DFAIT 13, Supplement 1 for remarking procedures.

Reliable Courier Service-

a courier or mail service whose reliability has been verified with other clients, the Better Business Bureau, or police authorities by DFAIT Distribution Services and which provides proof of mailing and on request, a record of transit and of delivery.

SECRET-

classification for information which could reasonably be expected to cause serious injury to the national interest if compromised.

Security Dispatch Case-

briefcase as listed in Security Equipment Guide SSB/SG-20 which has been tested and approved for transport of sensitive information and assets. Available to departmental employees as required from ISDF.

Security Zone-

is an area to which access is controlled and limited to authorized personnel and to authorized and properly-escorted visitors and only accessible through the Operations Zone. The Security Zone will be separated from the Operations Zone by a secure perimeter.

Sensitive Asset-

items, other than information, which have been identified as being important to operations by virtue of the function performed or as being valuable and therefore warrant safeguarding, (e.g. cash and other negotiable items) or computer systems that require protection to ensure the integrity and availability of the information stored therein.

Sensitive Information-

information which is either classified or designated and requires protection or special handling.

Tagged-

tag with name and address of sender or intended recipient which is applied to Security Dispatch Case when used to transport sensitive information or assets.

TRA-

Threat and Risk Assessment

TOP SECRET-

classification for information which could reasonably be expected to cause exceptionally grave injury to the national interest.

Transmission-

forwarding information via a number of methods such as, diplomatic bag, courier, mail, hand carriage or electronic means.

Transmit-

to transfer information and assets from one person or place to another by someone without a need-to-know the information or need-to-access the asset.

Transport-

to transfer sensitive information or assets from a controlled access area by an appropriately screened or cleared person with a need to know the information or access the asset to another appropriately screened or cleared person with a need to know the information or access the asset.

UNCLASSIFIED-

information which is not sensitive and does not require physical protective measures associated with designated or classified information.

TRANSMITTAL OF SENSITIVE

Transmit: To transfer sensitive information and assets from one person or place to another by someone without a need to know the information or need to access the asset.

MOVEMENT		CLASSIFICATION OR DESIGNATION OF INFORMATION
WITHIN L.B. PEARSON BUILDING		PROTECTED A PROTECTED B CONFIDENTIAL SECRET
		PROTECTED C
FROM DFAIT PREMISES IN A CONTROLLED ACCESS AREA[1] TO A CONTROLLED ACCESS AREA[1] INSIDE CANADA (e.g. Place Vanier, other Government Departments; company offices with security certification)	DFAIT SERVICES	PROTECTED A PROTECTED B
		CONFIDENTIAL SECRET
		PROTECTED C
Note : The preparation depends on the mail services used; DFAIT or external services (see last column). Contact DFAIT Disrtibution Services (SBG) to know the area they cover.	EXTERNAL SERVICES	PROTECTED A PROTECTED B CONFIDENTIAL SECRET
		PROTECTED C
FROM DFAIT TO DESTINATIONS OUTSIDE CANADA (OTHER THAN TO MISSIONS)		PROTECTED A PROTECTED B
FROM DFAIT HEADQUARTERS TO CANADIAN MISSIONS OR CONSULATES OR BETWEEN CANADIAN MISSIONS		PROTECTED A
		PROTECTED B CONFIDENTIAL
		PROTECTED C SECRET

Notes:

1. Controlled area : combination of the three zones- Operations Zone, Security Zone, and High Security Zone to which access is restricted.
2. Addressing: Normally address in non-specific manner but when necessary to restrict access add "...To be opened only by...(Name or position)".
3. Special transmittal method requests must be accompanied by - Authorization for use of Private Courier Service form (EXT 1223).

Caution : For handling procedures for Cabinet Documents, Top Secret or NATO information or assets see *Manual of Security Instructions* Chapter 2 or contact DFAIT Distribution Services (SBG).

INFORMATION AND ASSETS

USER PREPARATION OF DESIGNATED OR CLASSIFIED INFORMATION OR ASSETS	MAIL SERVICES TRANSMITTAL METHOD
SINGLE, ADDRESSED[1], ENVELOPE WITH COMPLETED EXT 106 STICKER (MAY BE STRING TIE ENVELOPE)	DFAIT DEPARTMENTAL MAIL OR MESSENGER SERVICE
DOUBLE ADDRESSED[2] ENVELOPES INNER -GUMSEALED ENVELOPE WITHCOMPLETED EXT 106 STICKER OUTER -WITHOUT SECURITY MARKING (MAY BE STRING TIE ENVELOPE)	
SINGLE, GUMSEALED ADDRESSED[2] ENVELOPE (ANNOTATE "BY HAND" WHEN REQUIRED) NO SECURITY MARKING	DFAIT DEPARTMENTAL MAIL, MESSENGER SERVICE OR BY HAND SERVICE
INDIVIDUAL DOCUMENTS IN SINGLE, GUMSEALED ADDRESSED[2] ENVELOPE (ANNOTATE "BY HAND" WHEN REQUIRED) NO SECURITY MARKING	
INDIVIDUAL DOCUMENTS IN DOUBLE GUMSEALED ADDRESSED[2] ENVELOPES INNER -WITH SECURITY MARKING OUTER -WITHOUT SECURITY MARKING (ANNOTATE "BY HAND" WHEN REQUIRED)	
SINGLE, GUMSEALED, ADDRESSED[2] ENVELOPE NO SECURITY MARKING	CANADA POST- 1ST CLASS OR RELIABLE COURIER SERVICE[4]
DOUBLE GUMSEALED ADDRESSED[2] ENVELOPES INNER - WITH SECURITY MARKING ENCLOSE COMPLETED TRANSMITTAL AND RECEIPT NOTE -EXT 34 OUTER -WITHOUT SECURITY MARKING	CANADA POST-REGISTERED MAIL OR RELIABLE COURIER SERVICE[4]
SINGLE, GUMSEALED ADDRESSED[2] ENVELOPE NO SECURITY MARKING	CANADA POST OR EQUIVALENT FIRST CLASS MAIL ABROAD
SINGLE, GUMSEALED ADDRESSED[2] ENVELOPE WITH SECURITY MARKING	DIPLOMATIC AIR FREIGHT
SINGLE, GUMSEALED ADDRESSED[2] ENVELOPE WITH SECURITY MARKING	DFAIT DIPLOMATIC COURIER BAG SERVICE
DOUBLE ENVELOPES INNER -GUMSEALED ADDRESSED[2] ENVELOPE WITH SECURITY MARKING AND SECURITY TAPE ENCLOSE COMPLETED RECEIPT FORM - EXT 34 OUTER -STRING TIE ENVELOPE ADDRESSED[2] TO "DFAIT Distribution Services " WITH COMPLETED EXT 106 STICKER	

TRANSPORT OF SENSITIVE

Transport: The transfer of sensitive information or assets from a controlled access area by an appropriately screened or cleared person with a need to know the information or access the asset to another appropriately screened or cleared person with a need to know the information or access the asset.

Notes:

1. Controlled Area: combination of the three - Operations Zone, Security Zone, and High Security Zone to which access is restricted.
2. Addressing - Normally address in non-specific way but when necessary to restrict access add...To be opened only by .. and name or position
3. Tag with full forwarding or return address and telephone number of carrier.
4. Contact the Management Services Unit (ISDF) for Security Dispatch Cases.

Caution : Whenever International boundaries are crossed, the use of DFAIT Diplomatic Bags is highly recommended. For handling procedures for Cabinet Documents, Top Secret or NATO information or assets see *Manual of Security Instructions* Chapter 2 or contact DFAIT Distribution Services (SBG).

DESTINATION
WITHIN L.B. PEARSON BLDG. WITHIN A CONTROLLED ACCESS AREA' (Within all towers and between towers A, B, and C when using interconnecting hallways)
WITHIN L.B. PEARSON BLDG. OUTSIDE A CONTROLLED ACCESS AREA' (when traversing public areas, main lobbies, basement corridors or garage)
FROM DFAIT HEADQUARTERS TO ANY DESTINATION INSIDE CANADA (e.g. Place Vanier, PWGSC HQ; Privy Council Office, other Government Departments. Document must remain under control of carrier at all times)
FROM CANADIAN DIPLOMATIC OR CONSULAR MISSION TO DESTINATION WITHIN HOST COUNTRY
FROM DIPLOMATIC OR CONSULAR MISSION TO DESTINATION OUTSIDE HOST COUNTRY

INFORMATION AND ASSETS

DESIGNATION OR CLASSIFICATION OF INFORMATION	APPROVED METHODS OF ENVELOPING AND ADDRESSING
PROTECTED A PROTECTED B CONFIDENTIAL	ENVELOPE NOT REQUIRED (TRANSPORT DISCREETLY)
PROTECTED C SECRET	SINGLE ENVELOPE NO SECURITY MARKING (MAY BE STRING TIE ENVELOPE)
PROTECTED A PROTECTED B PROTECTED C CONFIDENTIAL SECRET	SINGLE, ADDRESSED[2] ENVELOPE NO SECURITY MARKING (MAY BE STRING TIE ENVELOPE)
PROTECTED A PROTECTED B	SINGLE, ADDRESSED[2] ENVELOPE NO SECURITY MARKING (MAY BE STRING TIE ENVELOPE)
CONFIDENTIAL SECRET	SINGLE, GUMSEALED, ADDRESSED[2] ENVELOPE NO SECURITY MARKING
PROTECTED C	SINGLE, GUMSEALED, ADDRESSED[2] ENVELOPE WITH SECURITY MARKING AND ENCLOSED IN LOCKED TAGGED[3] BRIEFCASE
PROTECTED A PROTECTED B CONFIDENTIAL	SINGLE, GUMSEALED, ADDRESSED[2] ENVELOPE OR ENCLOSED IN LOCKED TAGGED[3] SECURITY DISPATCH CASE[4]
PROTECTED C SECRET	DOUBLE, GUMSEALED, ADDRESSED[2] ENVELOPES WITH SECURITY MARKING ON INNER ENVELOPE ONLY OR SINGLE, GUMSEALED, ADDRESSED[2] ENVELOPE WITH SECURITY MARKING AND ENCLOSED IN LOCKED TAGGED[3] SECURITY DISPATCH CASE[4]
PROTECTED A PROTECTED B PROTECTED C CONFIDENTIAL SECRET	SEE INSTRUCTIONS FOR TRANSMITTAL AND TRANSMIT BY DIPLOMATIC COURIER BAG OR CONTACT DFAIT DISTRIBUTION SERVICES (SBG) FOR AD-HOC COURIER SERVICE