LES NORMES DE SÉCURITÉ ET DE PROTECTION POUR LES INSTALLATIONS DU MAECI AU CANADA

AFFAIRES ÉTRANGÈRES ET COMMERCE INTERNATIONAL CANADA

ISC - Octobre 2006

ATML/DOC
.64203057(F)
.64203082(E)

NUMÉROS DE TÉLÉPHONE IMPORTANTS	
Vous avez besoin d'une nouvelle clé, d'un nouveau cadenas à combinaison ou à clé? Vous ne pouvez pas entrer dans votre bureau fermé à clé?	Envoyer un courriel à SPAS 992-6678 (Atelier de serrurerie de SPAS)
Vous avez besoin d'information sur la destruction de renseignements classifiés ou protégés?	992-6680 (SPAS)
Vous avez besoin d'une carte d'identité, d'un laissez-passer ou d'un laissez-passer temporaire?	(SPAS — Section de l'identité) 992-6691 (LBP BG-180)
Vous avez besoin d'une photo pour un passeport ou un visa?	(SERV/Section de l'identité) 944-3074
Vous avez perdu quelque chose?	944-0019 (SPAS)
Vous avez besoin d'information sur les cours, les séminaires, les séances d'information ou les outils de travail sur la sécurité?	992-6704 (ISC)
Vous avez des questions au sujet du processus d'enquête de sécurité?	992-6703, 992-6706, 944-1889, 992-1905 ou 992-3471

18-736-985(E)
18-736-987(F)

NUMÉROS DE TÉLÉPHONE D'URGENCE	
Ambulance	8+911
Service de police d'Ottawa	8+911
Service des incendies d'Ottawa	8+911
Poste de premiers soins de l'édifice LBP	992-1150
Centre de contrôle des mesures d'urgence de l'édifice LBP	992-1150
Commissionnaires (Bureau de la sécurité) de l'édifice LBP	992-5452
Chef des services de secours de l'immeuble de l'édifice LBP	992-5218
Chef adjoint des services de secours de l'immeuble de l'édifice LBP	992-6680
Mécanicien d'entretien de Travaux publics et Services gouvernementaux Canada	1-800-463-1850
Poste de premiers soins au 111 Sussex	944-2887
Centre de contrôle des mesures d'urgence au 111 Sussex	944-5555
Commissionnaires (Bureau de la sécurité) au111 Sussex	944-5551
Chef des services de secours de l'immeuble au 111 Sussex	992-5452
Chef adjoint des services de secours de l'immeuble au 111 Sussex	944-2597
Gestion immobilière (BLJC) au111 Sussex	8+241-8192
Centre antipoison	8+737-1100
Agent des affaires du travail — Développement des ressources humaines Canada	946-2800

TABLE DES MATIÈRES

À PROPOS DU PRÉSENT DOCUMENT

Le présent manuel a pour objectif de vous aider à vous acquitter de vos responsabilités en matière de sécurité à titre d'employé des Affaires étrangères Canada et Commerce international Canada (AEC et CICan)..

Depuis l'étiquetage, le traitement, l'entreposage, la transmission et la destruction de renseignements classifiés ou protégés en passant par l'utilisation de l'équipement sécuritaire et l'accès aux zones d'accès restreint, la sécurité constitue un élément important de vos décisions quotidiennes. Vos responsabilités à ce chapitre commencent dès votre arrivée au travail et se poursuivent même après que vous aurez quitté AEC et CICan.

Le présent manuel est un document de référence

La plupart des dispositions décrites dans le présent manuel, 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 (LBP) et au 111, promenade Sussex (ancien hôtel de ville) à Ottawa. Si vous travaillez dans un autre édifice à Ottawa ou ailleurs au Canada, y compris sur les lieux d'une conférence, vous devriez connaître les mesures de sécurité et d'urgence qui y sont en vigueur.

Étant donné que la plupart des renseignements contenus dans le présent manuel se rapportent à l'édifice LBP et au 111, promenade Sussex, il n'est pas censé remplacer la politique et les instructions plus détaillées établies par le Ministère. Vous êtes invité à vous reporter à l'ensemble complet des 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 la sécurité à la centrale et liaisons interministérielles (SPAS).

Si vous ne trouvez pas réponse à toutes vos questions dans le présent guide, ISC offre régulièrement des cours et des séances d'information. Communiquez avec la Section du personnel et de l'éducation en matière de sécurité (ISC) au 992-6704 pour obtenir le *calendrier des cours*.

INTRODUCTION

Affaires étrangères Canada et Commerce international Canada (AEC et CICan ou Ministère) 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 sauvegardées.

AEC et CICan possèdent 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 qui doivent être sauvegardés, de même que des documents de voyage comme des passeports, des visas et des permis ministériels.

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.

Il suffit souvent d'un peu de bon sens et de prévoyance pour assurer votre propre sûreté ainsi que la sécurité des renseignements et des biens.

MESURES DE SÉCURITÉ À L'ADMINISTRATION CENTRALE

La Section des opérations de la sécurité à la centrale et liaisons interministérielles (SPAS) est responsable de l'élaboration et de la mise en oeuvre de toutes les procédures, directives et instructions pour les situations où sont en jeu la sécurité du personnel ou la sauvegarde des biens du gouvernement, y compris les renseignements, à l'Administration centrale.

Procédures d'urgence de l'immeuble

Des procédures d'urgence simples élaborées pour l'édifice LBP et le 111 Sussex* sont consignées dans le *Manuel des instructions de sécurité* et dans le livret intitulé *Procédures d'urgence — Guide de l'employé*. Elles vous permettent de réagir d'une manière rapide, coordonnée et efficace dans diverses situations d'urgence, que ce soit un incendie, une urgence médicale ou une urgence grave touchant l'édifice.

Prenez le temps de lire le livret intitulé Procédures d'urgence — Guide de l'employé, *disponible à l'entrée des tours. On peut aussi consulter ce document dans le site Web du MAECI portant sur la sécurité :*
http://intranet/dfait-maeci.gc.ca/department/security/guides/emergproc-f.asp

Nota : Des mesures d'urgence adaptées au 111 Sussex sonts en vigueur.

Que faire en cas de perte ou de vol?

Protégez vos biens personnels en gardant en tout temps votre sac à main, votre portefeuille et votre argent, ainsi que tous les 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 de valeur comme les calculatrices, les ordinateurs (surtout les ordinateurs portatifs ou bloc-notes), les magnétophones ou les appareils photo : lorsque vous ne les utilisez pas, placez-les dans un classeur ou une pièce qui sont fermés à clé.

En cas de perte ou de vol, communiquez avec SPAS (Opérations de la sécurité) au 944-0019. Vous devez également signaler la perte ou le vol d'un bien du gouvernement à SRAA (Section de la gestion des locaux à la centrale) au 996-6816 et à SMSP (Section de la politique ministérielle, rapports et mise en oeuvre SIF) au 944-1102.

La sécurité physique à l'Administration centrale

La sécurité physique comprend toutes les mesures prises pour assurer la protection du personnel et la sauvegarde des renseignements et des biens, y compris :

- le contrôle quotidien de la circulation des personnes dans les zones d'accès restreint;
- les cartes d'identité et laissez-passer donnant accès à l'édifice;
- la surveillance par télévision en circuit fermé de certains point d'entrée et de sortie;
- les armoires métalliques de sûreté et autres classeurs approuvés;
- les chambres fortes;
- les déchiqueteurs approuvés;
- les systèmes d'alarme et matériel connexe;
- le contrôle radioscopique du courrier;
- les systèmes de contrôle d'accès et de détection des intrusions, et zones publiques, d'accueil, de travail, de sécurité et de haute sécurité.

Zones

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

Zone publique
Cette zone entoure les installations, ou en fait partie. Les cafétérias, les banques et les halls d'entrée sont des exemples de zones publiques.

Zone d'accueil
Située à l'entrée de l'édifice, cette zone 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.

Zones de travail
L'accès à ces zones est limité au personnel et aux visiteurs qui sont escortés par des employés détenant une cote de sécurité valide. Tous les pavillons et les tours sont des zones de travail.

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

Accéder à une zone — Laissez-passer

Des lecteurs de cartes magnétiques par glissement sont installés à l'entrée de chaque tour de l'édifice LBP et à divers endroits du 111 Sussex. Les employés doivent porter leur laissez-passer de manière à ce qu'il soit visible en tout temps lorsqu'ils sont dans ces immeubles ou dans d'autres installations du Ministère. Des laissez-passer ministériels avec photo des couleurs suivantes permettent d'accéder à l'édifice LBP et à 111 Sussex.

Laissez-passer bleu
Le laissez-passer bleu est délivré au personnel qui détient au moins une cote de sécurité de niveau II (SECRET). Il permet d'accéder aux zones d'accès restreint 24 heures par jour, 7 jours par semaine. Il permet également d'escorter des visiteurs ou des employés qui n'ont pas de laissez-passer pour les zones d'accès restreint du Ministère.

Laissez-passer vert
Le laissez-passer vert est délivré au personnel comme les employés nommés pour une période déterminée ou les employés contractuels qui détiennent au moins une cote de sécurité de niveau II (SECRET). Il permet de pénétrer sans escorte 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. Il ne permet pas d'escorter des visiteurs ou d'autres personnes sur les lieux.

Laissez-passer rouge
Le laissez-passer rouge est délivré au personnel non gouvernemental qui fournit des services au MAECI et n'a pas besoin de pénétrer dans les zones d'accès restreint. Ceux qui détiennent ce laissez-passer ne dispose pas d'une cote de sécurité et doivent être escortés dans les secteurs d'accès restreint.

Laissez-passer temporaire
Un laissez-passer temporaire n'est remis qu'au personnel disposant déjà d'un laissez-passer bleu ou vert et l'ayant oublié ou perdu. Le laissez-passer initial est désactivé lorsqu'on demande un laissez-passer temporaire et réactivé lorsqu'on le remet.

Laissez-passer rose
Le laissez-passer rose est délivré au personnel ayant une cote de fiabilité (autrefois appelée VAF). Ce laissez-passer est remis aux nouveaux employés en attente d'une cote de sécurité ou aux employés nommés à court terme comme les étudiants occupant un emploi d'été ou les employés contractuels.

Il permet seulement d'accéder à des zones d'accès restreint d'un immeuble spécifique (LBP, 111 Sussex, etc.). Un employé qui détient un laissez-passer rose est assujetti aux conditions suivantes :

- son accès est limité à une période ne dépassant pas six mois;
- il a accès aux documents de niveau Protégé A mais pas aux renseignements classifiés;
- il doit en tout temps être sous la supervision d'un employé ayant une cote de sécurité;
- il n'a pas de privilège d'escorte dans les zones d'accès restreint.

Le laissez-passer rose est délivré par SPAS suite à l'approbation par ISCT d'une cote de fiabilité.

Laissez-passer bordeaux
Un laissez-passer bordeaux n'est remis qu'aux employés du Haut Commissariat avec lesquels il y a une entente mutuelle.

Laissez-passer bleu/vert pour entrepreneur "C" (avec photo)
Remis aux fournisseurs de services et aux entrepreneurs chargés de l'entretien courant du matériel et des systèmes à l'AC du MAECI. Ces personnes doivent obtenir au préalable une autorisation de sécurité. Ces laissez-passer ressemblent à ceux des employés du Ministère, sauf que le nom de l'entreprise apparaît au-dessus d'un grand « C », à gauche de la photo. La couleur de la carte varie en fonction des privilèges d'accès du titulaire.

Laissez-passer temporaire « C » jaune
Remis aux entrepreneurs qui ont une autorisation de sécurité et qui doivent effectuer des travaux à l'AC du MAECI pendant une période déterminée. En raison de la durée limitée des travaux, il n'est pas nécessaire de leur remettre un laissez-passer pour entrepreneur « C » avec photo.

Nota : En ce qui concerne les autres bureaux du MAECI situés dans le SCN, il est possible de remettre un laissez-passer pour entrepreneur « C » avec photo à tout fournisseur de services qui répond à des besoins précis, peu importe l'endroit.

Seule l'apparence des laissez-passer temporaires pour entrepreneur peut changer en fonction de l'édifice où ils ont été délivrés ou du service de sécurité chargé de leur délivrance. On peut obtenir des précisions à ce sujet en communiquant avec les responsables de la gestion de l'édifice concerné.

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

Assurez la sécurité du Ministère et du lieu de travail en interpellant toute personne qui entre et qui n'est pas munie d'un laissez-passer lorsque vous employez votre carte pour entrer ou lorsque vous sortez d'une des tours. Communiquez immédiatement avec SPAS (992-5452) en cas de problème.

Comment obtenir un laissez-passer

Les laissez-passer ainsi que les cartes temporaires sont délivrés par SPAS qui est située au BG-180 (7 h à 14 h 45). Un laissez-passer ne sera autorisé qu'après vérification que le demandeur détient une cote de fiabilité ou une cote de sécurité. La prise d'empreintes digitales se fait également au même endroit.

Comment obtenir des passeports et des visas diplomatiques

Le service de photos pour les passeports et les visas diplomatiques est offert au Centre de services (SERV), pièce D1-423 de l'immeuble LBP, téléphone 944-3074, de 9 h à 11 h 30 et de 12 h 30 à 16 h 30. Pour toute question concernant les conditions d'obtention d'un passeport officiel, les détails sur les visas ou le temps requis pour le traitement, veuillez communiquer avec JWC au 994-3550 (téléphone) ou au 997-1255 (télécopieur).

Pour obtenir des photos, une confirmation d'affectation ou un formulaire d'autorisation de voyage est nécessaire. Pour les cas spéciaux, veuillez faire parvenir un courrier électronique à Ann Séguin-Huskas (SPAS).

Laissez-passer de visiteur

Les visiteurs qui ne possède pas de carte d'identité valide du MAECI se rerront remettre un laissez-asser en échange d'une carte d'identité avec photo. Ils devront mettre ce laissez-passer en évidence tout au long de leur visite. Il existe deux types de laissez-passer de visiteur:

Laissez-passer jaune

Un laissez-passer jaune est remis aux visiteurs dont la cote de sécurité, Secret à minimum, a été confirmée par SPAS et enregistrée dans le SIPV. Les visiteurs qui reçoivent un laissez-passer jaune peuvent se déplacer dans l'édifice sans être accompagnés. Les commissionnaires informeront les employés concernés de l'arrivée de leurs invités.

Laissez-passer rouge

Un laissez-passer rouge est remis aux visiteurs dont la cote de sécurité n'a pas été vérifiée. Les visiteurs qui se verront délivrer un laissez-passer rouge devront être accompagnés en tout temps dans l'édifice. Les commissionnaires informeront les employés concernés de l'arrivée de leurs invités. Une fois la visite confirmée, ils accompagneront les visiteurs à leur destination. Le personnel du Ministère devra raccompagner les visiteurs jusqu'u hall d'entrée principal à leur départ.

La pratique actuelle consistant à inscrire les visiteurs à l'avance se poursuivra. Il s'agira de communiquer avec le bureau principal de la réception par courrier à DFAIT Front desk/Réception MAECI-SPAS et de fournir l'information relative aux réunions et aux personnes qui y assistent.

Une fois la visite terminée, il vous incombe d'escorter ces visiteurs vers une zone publique ou de faire en sorte qu'une autre personne les escorte vers cette zone. Cela vaut aussi pour les individus de l'extérieur qui participent à des réunions à l'édifice LBP ou au 111 Sussex.

Services du bureau d'accueil à l'Administration centrale

Les membres du personnel du bureau d'accueil des AEC et CICan peuvent accueillir vos invités et visiteurs plus rapidement et efficacement au moyen des données des Profils dans les Applications ministérielles. Ils doivent pouvoir communiquer avec vous par téléphone lorsque vos invités arrivent.

Veuillez vous assurer que les données dans votre profil sont à jour, par exemple, les numéros de bureau et de téléphone, en consultant la Base de données — Profils dans les Applications ministérielles. Pour plus amples renseignements, consultez le document suivant : http://intranet.lbp/department/sxd/howTo/genpro-f.asp

Veuillez informer SPAS lorsque vous attendez des visiteurs. Cela peut se faire de trois manières :

1. Courrier électronique : bureau d'accueil des AEC et CICan — SPAS (reception@dfait-maeci.gc.ca).
2. Messagerie vocale : 995-5859.
3. Liste des visiteurs attendus remise au bureau d'accueil.

Accéder à une zone d'accès restreint en dehors des heures normales de travail (sur semaine entre 16 h et 8 h, les fins de semaine et les jours fériés)

Même s'il existe des lecteurs de cartes magnétiques, il est conseillé de signer le registre à votre arrivée et à votre sortie des édifices en dehors des heures normales de travail. C'est un moyen de savoir quels employés sont sur place et l'endroit où ils se trouvent en cas d'urgence.

Le système d'alarme en dehors des heures normales de travail

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

Stationnement

Les permis de stationnement sont délivrés par la Direction des services administratifs (SPAA) de l'Administration centrale, située au rez-de-chaussée de la tour D de l'édifice LBP. Si vous avez des questions concernant ces permis, communiquez avec SPAA (992-2338). SPAS, par un accord spécial avec la GRC, applique les règlements sur le stationnement établis dans le *Règlement relatif à la circulation sur les terrains du gouvernement.*

Responsabilités du Corps canadien des commissionnaires

Le Corps canadien des commissionnaires assure des services de sécurité pour l'édifice LBP et le 111 Sussex. Ces commissionnaires peuvent exiger la présentation de cartes d'identité. Ils sont chargés des tâches suivantes :

- assurer la réception et contrôler l'accès;
- contrôler les systèmes d'alarme des édifices et intervenir au besoin;
- mener des patrouilles de sécurité et des rondes d'incendie;
- contrôler l'entrée des visiteurs et les escorter jusqu'au bureau d'un employé après avoir communiqué avec ce dernier;
- surveiller le matériel qui entre dans l'édifice LBP et le 111 Sussex, et qui en sort.

IDENTIFICATION ET SAUVEGARDE DE L'INFORMATION

La Politique de sécurité du gouvernement établit un cadre de directives concernant le respect des exigences en matière de sécurité de l'information et de protection des renseignements personnels. Ce cadre oblige le Ministère à sauvegarder de façon adéquate les renseignements personnels et autres données de nature délicate contenus dans ses systèmes d'information ou utilisés pour la prestation de ses programmes et services. 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 sauvegarder les renseignements et les biens que vous utilisez 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 des intérêts privés ou non reliés à l'intérêt national dont le Parlement assume la responsabilité.

Il existe trois niveaux de confidentialité des renseignements :
1. renseignements non classifiés;
2. renseignements protégés;
3. renseignements classifiés.

Pendant vos activités quotidiennes, assurez-vous d'être en mesure de déterminer quels renseignements sont classifiés ou protégés, de choisir le niveau de confidentialité approprié et de marquer ces renseignements de façon adéquate (par exemple, Secret, Protégé A, etc.) afin que les tiers sachent qu'il faut appliquer des mesures de protection spéciales.

Vous devriez également pouvoir :
- choisir de l'équipement sécuritaire et un emplacement sûr pour produire de tels renseignements, en discuter ou les transmettre;
- stocker les renseignements de façon sûre;
- détruire les renseignements de façon sûre.

Identification des renseignements classifiés et protégés

Tous les renseignements n'ont pas à être classifiés ou protégés. 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 de sécurité du gouvernement, il vous incombe de préciser le niveau de confidentialité des renseignements que vous produisez.

Les renseignements et les biens du Ministère doivent au moins faire l'objet d'une attention raisonnable qui est conforme aux pratiques administratives de base. Il ne faut jamais classifier ou protéger 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.

Renseignements classifiés

Les renseignements sont classifiés si leur divulgation peut nuire à l'intérêt national du Canada, c'est-à-dire la défense et la conservation de la stabilité sociale, politique et économique du Canada. Il y a trois niveaux de classification :

1. **Très Secret** — lorsque la compromission de l'information pourrait vraisemblablement causer un **préjudice exceptionnellement grave** à l'intérêt national, par exemple :
   - information sur un risque de conflit armé touchant le Canada ou ses alliés;
   - information sur des services de renseignement;
   - rapports dont la diffusion pourrait entraîner la mort ou la torture d'une personne.

2. **Secret** — lorsque la compromission de l'information pourrait vraisemblablement causer un **préjudice grave** à l'intérêt national, par exemple :
   - procès-verbaux des réunions du Cabinet ou des comités du Cabinet;
   - informations sur d'importantes négociations internationales;
   - informations ayant trait à la sécurité fédérale-provinciale ou nationale.

3. **Confidentiel** — lorsque la compromission de l'information pourrait vraisemblablement causer un **préjudice** à l'intérêt national, par exemple :
   - procès-verbaux des réunions des comités interministériels;
   - instructions sur la sauvegarde de renseignements hautement classifiés;
   - rapports de missions qui pourraient influer sur les relations internationales.

Renseignements protégés

Les renseignements protégés sont de nature délicate lorsque leur compromission pourrait causer un préjudice à des intérêts privés ou non reliés à l'intérêt national dont le gouvernement assume la responsabilité. L'information est délicate, mais elle n'influe pas sur l'intérêt national. Il y a trois niveaux de protection :

1. **Protégé C** — lorsque la compromission de l'information pourrait vraisemblablement causer un **préjudice potentiellement élevé** à des intérêts non reliés à l'intérêt national comme la sécurité des personnes; par exemple, les renseignements commerciaux importants ou l'application de la loi.

2. **Protégé B** — lorsque la compromission de l'information pourrait vraisemblablement causer un **préjudice potentiellement moyen** à des intérêts privés ou non reliés à l'intérêt national, notamment un tort ou un embarras durables qui auront des effets négatifs sur la carrière ou la réputation d'une personne, par exemple le secret professionnel de l'avocat, les renseignements commerciaux ou les évaluations du personnelle.

3. **Protégé A** — lorsque la compromission de l'information pourrait vraisemblablement causer un **préjudice potentiellement bas** à des intérêts non reliés à l'intérêt national, par exemple la divulgation du salaire exact d'une personne ou d'un numéro d'assurance sociale.

Renseignements provenant d'autres organismes

Les renseignements reçus d'un autre échelon de gouvernement au Canada, de gouvernements étrangers ou d'organismes internationaux doivent être sauvegardés conformément aux niveaux de protection accordés par l'organisme responsable. Par exemple, si vous élaborez une note d'information concernant un document classifié SECRET, vous donnez tout simplement une classification SECRET à la note d'information.

Le *Guide de classification et de protection* fournit des instructions sur la façon de marquer les documents suivants :	
• bibliographies et références • information d'une tierce personne • films et négatifs • chemises de classement	• documents de l'OTAN • documents destinés à une diffusion externe • documents avec mention de mise en garde

Pour plus d'informations, veuillez consulter notre site Web :
http://intranet.dfait-maeci.gc.ca/department/security/menu-f.asp

Déclassification ou déclassement automatiques

Les renseignements ne sont classifiés ou protégés que pour la période pendant laquelle ils doivent être sauvegardés. Après cette période, la classification ou la protection 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, par exemple :

- Confidentiel (non classifié à compter du 31 juillet 2002);
- Protégé A (non classifié si l'annexe A est retirée).

Modification du niveau de la classification ou de la protection d'un document

Si vous voulez modifier le niveau de la classification ou la protection 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 protection doivent être inscrits lisiblement à l'encre à la marge de droite dans le haut de la page sur le document.

Vous devez faire tout votre possible pour obtenir la participation de l'auteur du document avant de modifier son niveau de classification ou protection, 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 exemple, 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 protection 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 à la Direction des relations avec les médias (BCM) ou au bureau du Coordonnateur de l'accès à l'information et de la protection des renseignements personnels (DCP).

Traitement du matériel classifié ou protégé

De nombreux documents entrent au Ministère ou en sortent. Certains sont de nature plus délicate que d'autres et exigent des procédures spéciales. Pour plus amples renseignements, voir les appendices (disponibles à l'entrée des tours et pavillons) indiqués dans le tableau suivant.

Normes pour la transmission (voir l'appendice A)	***Normes pour le transport*** (voir l'appendice B)
Transfert de renseignements et de biens classifiés ou protégés par une personne n'ayant pas « besoin de connaître » leur contenu.	Transfert PAR PORTEUR de renseignements et de biens classifiés ou protégés par un employée du ministère ayant une cote de sécurité appropriée et un besoin de connaître leur contenu.

Téléphones et télécopieurs protégés

Un téléphone protégé, appelé STU-III, fournit un moyen de communication téléphonique protégé au personnel qui a besoin de transmettre des renseignements classifiés ou protégés 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.

Nota : Le terminal, pris isolément, est NON CLASSIFIÉ. La clé d'activation cryptographique (CAC), prise isolément, est aussi NON CLASSIFIÉE. Toutefois, une fois la clé insérée dans le terminal, l'appareil est CLASSIFIÉ.

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

- lorsqu'une CAC ou un terminal STU-III est perdu ou volé;
- lorsqu'une CAC a été laissée dans un terminal sans surveillance;

- lorsqu'un STU-III semble avoir été soumis à des interventions abusives.

L'équipement nécessaire à la transmission protégée de documents (jusqu'au niveau Secret) par *télécopieur* est disponible dans de nombreux bureaux. Les contrôles sont semblables à ceux employés pour les téléphones STU-III.

Dans certaines conditions, vous pouvez être autorisé à recevoir ou à entendre des renseignements classifiés ou protégés au moyen d'un STU-III, mais à parler seulement à un niveau non classifié.

Rangement du matériel classifié ou protégé

Vous devez assurer EN TOUT TEMPS la sauvegarde des renseignements classifiés ou protégés qui se trouvent en votre possession.

N'oubliez pas que plus de 40 000 personnes visitent la centrale des AEC et CICan chaque année. Donc, lorsque vous vous absentez de votre bureau pour une période prolongée, fermez la porte à clé; si vous travaillez dans une aire ouverte, rangez le matériel classifié ou protégé dans un endroit sûr.

Discussion des renseignements classifiés ou protégés

- Vous ne devez pas discuter de renseignements classifiés ou protégés dans un endroit public ni sur une ligne téléphonique non protégée.

- Lorsque vous discutez de renseignements classifiés ou protégés avec quelqu'un, assurez-vous que votre interlocuteur en connaît le niveau de classification ou protection et qu'il possède le niveau d'autorisation approprié.

- Dans le cas d'une conférence ou d'un autre événement public, les participants doivent être informés au début et à la fin de l'événement que les sujets abordés peuvent être classifiés ou protégés et spécifiés à quels niveaux.

Exigences minimales pour le rangement du matériel classifié ou protégé

Les exigences minimales pour le rangement du matériel classifié ou protégé au Canada sont les suivantes :

Très Secret
Doit être rangé dans un coffre-fort approuvé dans une zone de haute sécurité.

Confidentiel, Secret, Protégé A, B et C
Peut être rangé dans une zone de travail dans un classeur de sécurité muni d'un moraillon double et d'un cadenas à combinaison approuvé.

Changement d'une 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;
- lors de l'embauche d'un nouvel employé;
- lorsque la combinaison est ou a peut-être été compromise.

Il faut envoyer la demande de changement de combinaison à SPAS par courrier électronique.

Clés des bureaux

L'adjointe administrative 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 l'adjointe administrative ou à l'employé responsable des clés dans votre section d'ouvrir la porte. Si aucun d'eux n'est disponible, téléphonez à l'atelier de serrurerie de SPAS (992-6678) pour faire ouvrir la porte. Le délai d'intervention dépend de la disponibilité du personnel.

- Sauvegardez vos clés en tout temps.
- Ne faites pas un double de vos clés; les clés de rechange sont contrôlées par l'adjointe administrative de section ou une personne désignée.
- L'adjointe administrative peut obtenir une nouvelle clé en faisant parvenir un courrier électronique à l'atelier de serrurerie de SPAS.

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

Utilisation des cartes d'absence

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

Si vous prévoyez vous absenter, contactez SPPM pour obtenir une carte d'absence et placez-la sur votre bureau. Ne laissez jamais de matériel ou de documents classifiés ou protégés sur votre bureau.

Travail à la maison avec du matériel classifié ou protégé

Vous devez parfois travailler avec du matériel classifié ou protégé le soir ou la fin de semaine, mais il n'est pas recommandé d'apporter ce genre de document à la maison ou à quelque autre endroit que ce soit. Dans certains cas cependant, à Ottawa, le directeur peut en accorder la permission.

La permission peut être accordée si les conditions suivantes sont respectées :
- il est interdit d'apporter des renseignements TRÈS SECRETS;
- vous êtes personnellement responsable de la garde du matériel; et
- le matériel doit être sauvegardé en tout temps.

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

Élimination des renseignements classifiés ou protégés

Les documents classifiés (Confidentiel et Secret) et protégés (Protégé A, B et C) doivent être éliminés à l'aide des déchiqueteurs qu'on trouve sur tous les étages. Si vous avez un volume important de documents de rebut classifiés (par exemple, si votre direction déménage ou doit mettre au rebut des documents Très Secrets), envoyez un courrier électronique à SPAS pour les faire ramasser ou pour obtenir des directives. Les documents non classifiés doivent être recyclés.

Incidents de sécurité (Infractions et manquements à la sécurité)

Une **infraction** est une divulgation non autorisée de renseignements classifiés ou protégés, ou un accès sans autorisation à ces renseignements. Il peut s'agir aussi de la perte ou du vol d'un équipement ou de matériel protégé 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 mis dans l'embarras 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 les procédures de sécurité, ce qui risque d'occasionner une infraction à la sécurité. Il y a manquement dans les circonstances suivantes :

- des renseignements ne sont pas classifiés ou protégés conformément à la Politique de sécurité du gouvernement;
- des renseignements sont classifiés ou protégés en contravention à la Politique de sécurité du gouvernement;
- des renseignements ou des biens classifiés ou protégés sont modifiés, conservés, divulgués ou enlevés sans autorisation;
- des renseignements ou des biens classifiés ou protégés ne sont pas sauvegardés; ou
- des renseignements classifiés ou protégés à un niveau supérieur à Protégé A ont été traités sur SIGNET 3.

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 classifiés ou protégés sont laissés sans protection adéquate, ou encore que des clés ou des cadenas 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 ISC.

Lorsqu'un commissionnaire trouve du matériel non protégé, ce matériel peut être saisi et détenu par SPAS. 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 SPAS, lorsque vous récupérez l'information visée par l'infraction.

Conseils pour sauvegarder le matériel classifié ou protégé

- Prenez l'habitude de ranger votre bureau; le jour, placez le matériel classifié ou protégé seulement sur votre table de travail, et non sur les classeurs, sur le bord des fenêtres ou dans un tiroir.
- À la fin de la journée, faites une inspection visuelle de votre bureau.
- Présumez toujours que vous ne retournerez pas à votre bureau lorsque vous partez en réunion; rangez donc tout le matériel classifié ou protégé dans votre classeur.
- Laissez une carte d'absence sur votre bureau.
- Fermez toujours votre bureau à clé lorsque vous quittez pour la journée ou pour assister à une réunion.

Sanctions à la suite d'infractions ou de manquements à la sécurité

Le sous-ministre a le droit d'appliquer des sanctions administratives ou disciplinaires à la suite d'infractions ou de manquements. Les sanctions peuvent prendre les formes suivantes :

- une réprimande verbale ou écrite;
- la révocation de la cote de fiabilité ou le déclassement ou révocation de la cote de sécurité;
- la suspension sans solde;
- le congédiement; ou
- une accusation au criminel.

Comment 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 qui sont entrés et sortis, de même que le nom de l'agent responsable de leur sécurité, sont consignés dans le registre de la Direction de la liaison avec le Cabinet et des Affaires parlementaires (DCL). Un système de rappel est également en place, de sorte qu'un rappel est envoyé aux agents lorsque la date de retour est imminente.

Les règlements du Conseil privé exigent que les documents du Cabinet qui sont fournis à des fins ministérielles doivent être retournés à DCL dans un délai déterminé, surtout à la fin d'une session parlementaire lorsque les réunions hebdomadaires du Cabinet prennent fin.

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.

Les sections qui pourraient avoir besoin de ces documents, par exemple au cours de l'été, peuvent prendre des dispositions pour que les documents qui ont été retournés à DCL puissent être distribués de nouveau.

VÉRIFICATION DE SÉCURITÉ DU PERSONNEL

Accès aux biens du gouvernement (y compris les renseignements)

Le principe du « besoin de connaître » est un élément important et fondamental d'un bon système de sécurité. Il s'agit de limiter l'accès aux renseignements ou aux biens protégés ou classifiés aux personnes qui doivent en prendre connaissance dans l'exercice de leurs fonctions. Aucun employé n'a le droit de prendre connaissance ou d'avoir la garde de renseignements classifiés ou protégés uniquement parce qu'il détient une cote de sécurité.

Tous les employés du Ministère doivent faire l'objet d'une vérification de sécurité avant d'être nommé à un poste.

Il y a deux sortes d'enquête de sécurité :
- la vérification de la fiabilité;
- l'évaluation de sécurité.

Pour avoir accès aux biens du gouvernement, y compris aux renseignements, vous DEVEZ détenir une cote de fiabilité valide.

La cote de fiabilité

Avant qu'une personne soit nommée à un poste, une vérification de sa fiabilité doit être menée et elle doit obtenir une cote de fiabilité. Une personne ayant obtenu une cote de fiabilité peut avoir accès à des renseignements et des biens non classifiés et protégés.

La vérification et la validation des éléments suivants sont nécessaires :
- ❑ renseignements de nature personnelle et professionnelle;
- ❑ études et qualifications professionnelles;
- ❑ accréditations ou certifications;
- ❑ références;
- ❑ casier judiciaire;
- ❑ cote de solvabilité;
- ❑ vérification dans le fichier nominatif (filtrage) s'il y a lieu.

Une fois la vérification de la fiabilité effectuée, on peut avoir accès aux renseignements protégés (Protégé A, B et C) suivant le principe du « besoin de connaître ».

Vérification de la fiabilité : procédures (condition préalable à une cote de sécurité)

Avant de nommer un nouvel employé, le gestionnaire responsable ou l'agent de dotation doit envoyer les formulaires suivants par la poste ou par porteur pour effectuer une vérification de la fiabilité.

Formulaires requis
❑ Formulaire de vérification de sécurité, de consentement et d'autorisation du personnel(TBS/SCT 330-23). ❑ Formulaire d'autorisation de sécurité (TBS/SCT 330-60)- pour toutes cote de sécurité. ❑ Formule pour la prise d'empreintes digitales qui se fait à la Section d'identité de SPAS (seulement pour cote de sécurité Très Secret ou à la demande de ISCT). *On peut se procurer tous ces formulaires, outre la formule d'empreintes digitales, au moyen de l'Intranet, services, formulaires en direct.*

Procédures pour remplir le Formulaire de vérification de sécurité, de consentement et d'autorisation du personnel TBS/SCT 330-23

1. Dans la partie supérieure du formulaire, indiquer s'il s'agit d'une nouvelle demande ou d'une demande de reclassement. Indiquer aussi s'il s'agit d'une demande de vérification de la fiabilité.

2. **Partie A :** La partie A doit être remplie par la personne faisant l'objet de l'enquête de sécurité. Elle doit s'assurer de fournir tous ses prénoms et noms de familles (y compris son nom de jeune fille, son patronyme ou matronyme et un changement de nom s'il y a lieu) puisque l'enquête relative à l'existence d'un casier judiciaire portera sur tous ces noms.

3. **Partie B :** « Détails relatifs à la nomination ». Donner tous les renseignements concernant le poste visé. Donner le nom et l'adresse du « Demandeur », ainsi que ses numéros de téléphone et de télécopieur.

4. **Partie C :** « Évaluation de la vérification et consentement ». La personne faisant l'objet de l'enquête doit signer et dater le formulaire et parapher les cases de 1 à 4 dans la colonne Y. Il faut demander à ISCT de confirmer l'attribution de la cote de fiabilité.

5. S'assurer que la personne faisant l'objet de l'enquête de sécurité consent aux procédures suivantes :
   - consentement à la divulgation et à la vérification subséquente, en paraphant toutes les cases;
   - consentement écrit, en signant et en datant la partie C du formulaire.

6. Une fois que la personne faisant l'objet de l'enquête a consenti aux vérifications, suivre la procédure suivante.

Processus de vérification de la fiabilité *(Partie C, case 1)*

Vérifications à être effectuées par le gestionnaire responsable ou l'agent de dotation

1. Preuve d'identité (données personnelles)
   Partie C (Inspection des documents, c'est-à-dire : certificat de naissance, passeport et photographie)
   But : Empêcher l'usurpation d'identité et s'assurer que les documents sont bien ceux de la personne faisant l'objet de l'enquête.

2. Études
   Partie C (Inspection des diplômes et des certificats, et vérification auprès de l'établissement d'enseignement)
   But : S'assurer que la personne faisant l'objet de l'enquête dit la vérité sur ses antécédents. Vérifier la date des études et les diplômes obtenus. Vérifier s'il s'agit d'un établissement d'enseignement reconnu ou d'une société qui vend des diplômes par correspondance.

3. Antécédents professionnels (période de cinq ans)
   Partie C (Un appel téléphonique auprès des employeurs antérieurs est suffisant.)
   But : Déterminer la fiabilité de la personne faisant l'objet de l'enquête dans ses emplois antérieurs et s'assurer qu'elle dit la vérité sur ses antécédents. Il est recommandé de couvrir une période de cinq ans. Si la personne concernée a occupé six emplois au cours des cinq dernières années, téléphonez aux six employeurs.

4. Références (période de cinq ans)
   Partie C (Remplir cette section en même temps que celle portant sur les antécédents professionnels)
   But : Déterminer si la personne faisant l'objet de l'enquête a été honnête, digne de confiance et fiable dans le passé. Il faut questionner les personnes concernées sur leur connaissance de la personne faisant l'objet de l'enquête de même que sur ses antécédents et son caractère.

Sections à remplir par ISCT

5. Vérification du casier judiciaire
   Partie C, case 2
   But : Déterminer si la personne faisant l'objet de l'enquête a commis des crimes dans le passé qui comporteraient un risque inacceptable par rapport aux fonctions à être remplies. Il s'agit de déterminer si cette personne a été un délinquant primaire ou un récidiviste, si les crimes ont été commis récemment, et de quelle manière les crimes sont liés aux exigences de l'emploi.

6. Enquête sur la solvabilité
   Partie C, case 3
   But : Déterminer si la personne faisant l'objet de l'enquête pourrait être sujette à des

pressions financières susceptibles d'influer sur le degré de confiance nécessaire par rapport aux fonctions à remplir. Cette question est particulièrement importante si l'employé doit s'occuper de gérer des fonds publics ou des bases de données financières, ou faire l'acquisition de biens ou de propriétés ainsi que l'achat de fournitures.

7. TRANSLATE FROM ENGLISH
Partie C, case 4

8. Vérification dans le fichier nominatif (filtrage) par le SCRS
Partie C, case 5
But : Déterminer s'il y a des raisons national liées à la sécurité pour refuser un emploi à la personne concernée.

Seulement que préalable à l'approbation obtenu du Secrétariat du Conseil du Trésor du Canada, la case 5 serait t-elle utilisée.

En vertu de la Politique de sécurité du gouvernement, l'accès aux renseignements et aux biens classifiés est réservé aux personnes ayant fait l'objet d'une évaluation de sécurité et ayant reçu une cote de sécurité au niveau approprié. IL OU ELLE NE DOIT PAS être nommé à un poste nécessitant un accès à des renseignements et à des biens classifiés avant que la cote de sécurité ait été attribuée.

La cote de sécurité

La cote 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. L'évaluation nécessaire pour l'obtention d'une cote de sécurité s'ajoute à la vérification de la fiabilité. Elle porte sur :

- les références concernant la réputation;
- les antécédents personnels, pouvant couvrir une période de 10 ans ou plus;
- les fichiers du Service canadien du renseignement de sécurité (SCRS).

Il existe trois niveaux de cote de sécurité, qui correspondent aux trois niveaux de documents classifiés :	
Niveau I	Accès aux documents ne dépassant pas le niveau CONFIDENTIEL
Niveau II	Accès aux documents ne dépassant pas le niveau SECRET
Niveau III	Accès aux documents ne dépassant pas le niveau TRÈS SECRET

Généralement, il faut une cote de sécurité de niveau II (SECRET) pour travailler à l'Administration centrale.

Les membres du service extérieur permutant affectés à l'étranger doivent détenir obligatoirement une cote de sécurité de niveau III (TRÈS SECRET).

Mariage ou cohabitation

Si vous détenez une cote de sécurité approprié 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 ISCT pour vérification. D'après les renseignements que vous aurez fournis, une évaluation de sécurité sera menée afin de déterminer s'il y a des informations concernant votre conjoint éventuel indiquant que vous pourriez agir contre l'intérêt national.

Comportement

La plupart des questions personnelles n'influent pas sur les intérêts du Ministère en matière de sécurité. Toutefois, certaines activités, notamment lorsqu'une personne est à l'étranger, pourraient la rendre susceptible aux menaces ou au chantage ce qui pourrait constituer une menace à la sécurité du Canada ou à la sécurité de renseignements classifiés dans l'intérêt national.

Voici des exemples de ce genre d'activités :

- ❑ abus d'alcool;
- ❑ mauvaise gestion de ses finances personnelles;
- ❑ utilisation de drogues à des fins non médicales;
- ❑ problèmes personnels qui pourraient influer sur la cote de sécurité;
- ❑ fréquentation suspecte de ressortissants étrangers ou d'organisations criminelles.

Tous les employés devraient bien connaître et se conformer au Code de conduite du Ministère qui se trouve à :

http://intranet.dfait-maeci.gc.ca/department/SPD/HRmanual/fchap2.htm

Déclassement ou révocation d'une cote de fiabilité ou d'une cote de sécurité

À la suite d'une révision fondée sur des renseignements défavorables concernant une personne, celle-ci peut se voir révoquer sa cote de fiabilité ou déclasser ou révoquer sa cote de sécurité.

Le pouvoir de réviser, révoquer, suspendre ou déclasser les cotes de sécurité appartient à l'administrateur général qui ne peut pas le déléguer.

Le pouvoir de réviser, révoquer ou suspendre les cotes de fiabilité appartient au gestionnaire délégué.

Dans les deux cas, l'intéressé est avisé de son droit de recours et privé de l'accès aux renseignements et biens classifiés ou protégés.

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION (TI)

La sécurité de la technologie de l'information (TI) sauvegarde les systèmes, les biens, les renseignements et les services ministériels contre des menaces délibérées ou accidentelles, en vue de garantir :

- la confidentialité des renseignements;
- l'intégrité des processus et des données;
- la disponibilité des données, des systèmes et des services.

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 ce matériel.

La TI comprend aussi tous les renseignements et données que vous créez dans le cadre de vos fonctions; les rapports officiels, les notes de service, les messages de courrier électronique, etc. sont des documents gouvernementaux et appartiennent à l'État.

Pourquoi la sécurité de la TI est-elle nécessaire?

Les employés d'AEC et de CICan doivent se protéger contre plusieurs menaces à la sécurité de la TI, notamment :

- des menaces *délibérées* y compris l'accès non autorisé à des données ministérielles, l'écoute électronique, l'inobservation des pratiques d'AEC et de CICan et les virus;
- des actions ou des événements *accidentels* y compris les erreurs des utilisateurs, l'ignorance des utilisateurs et la défaillance du matériel informatique.

Réseaux ministériels

Les réseaux ministériels suivants sont utilisés pour traiter l'information :

- SIGNET 3 (autrefois SIGNET 2000+)
- SIGNET 2000+ (autrefois SIGNET D)
- SIGNET C4.

SIGNET 2000+/SIGNET 3

Le SIGNET 2000+/SIGNET 3 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 protection n'est pas supérieure à Protégé A. Tous les employés ont accès à ce système, y compris les employés recrutés sur place, ainsi que quelques ministères, d'autres organismes et des gouvernements étrangers. Dans la plupart des missions, un administrateur de système recruté sur place est responsable du sytème SIGNET 2000+/SIGNET 3.
Note: Tout personnel doit, au minimum, tenir une cote de fiabilité avant avoir accès à SIGNET 2000+/SIGNET 3.

Traitement des données classifiées ou protégées

Vous devez connaître le matériel TI à utiliser pour chacun des niveaux de renseignements protégés ou classifiés. Voici deux principes dont il faut tenir compte :

1. Le matériel TI du Ministère est approuvé pour traiter des renseignements jusqu'à un niveau de protection maximale, c'est-à-dire que les mesures de sécurité du matériel assurent un niveau de protection approprié des renseignements suivant le degré de sensibilité de ceux-ci.

2. Le niveau de protection ou de classification de l'information détermine le matériel TI à utiliser.

La règle générale est la suivante : il faut utiliser un système TI dont les mesures de sécurité concordent avec le niveau de classification des renseignements. Si vous avez à faire usage de matériel TI pour traiter des renseignements du niveau Protégé B jusqu'au niveau Secret, utilisez SIGNET C4.

SIGNET C4

Le système SIGNET C4 est distinct et différent de SIGNET 2000+. Ce réseau peut être utilisé par les employés détenant une cote de sécurité de niveau II (Secret) au minimum et qui ont besoin de traiter et transmettre des renseignements dont la classification n'est pas supérieure à SECRET. Comme on utilise le système SIGNET C4 pour les données d'une nature plus délicate, il comporte des dispositifs de sécurité supplémentaires, notamment :

- un disque dur amovible qu'on peut ranger lorsque les lieux sont laissés sans surveillance; et
- un dispositif de cryptage approuvé;

N'oubliez pas qu'aucun mode électronique de traitement, de stockage, de transmission ou de communication de renseignements n'est sûr, sauf si on utilise du matériel ou des systèmes approuvés, conformément aux normes et aux procédures de sécurité.

Conseils pour l'utilisation des réseaux

- Joignez une étiquette indiquant le niveau de classification ou de protection à tous les messages imprimés, stockés ou transmis.
- Effectuez une fermeture de session sur votre poste de travail (SIGNET 2000+/SIGNET 3 et C-4 lorsque vous le laissez sans surveillance.
- Utilisez des logiciels approuvés sur les serveurs et les postes de travail.
- N'installez pas de modem et n'établissez pas de connexions avec d'autres ordinateurs ou réseaux, sauf si votre administrateur de système vous y a autorisé.

Votre mot de passe

Votre mot de passe, c'est vous. C'est une mesure de sécurité pour VOUS protéger, ainsi que VOTRE IDENTITÉ. C'est aussi la mesure de sécurité adoptée par AEC et CICan pour empêcher un accès non autorisé à ses systèmes. Ne révélez jamais votre mot de passe à qui que ce soit — une personne utilisant votre mot de passe peut se faire passer pour vous, ce qui peut avoir des conséquences graves pour votre carrière, ainsi que pour la sécurité d'AECet de CICan.

Lorsque vous vous absentez, utilisez la fonction permettant de faire suivre le courrier automatiquement à un collègue, ou utilisez la fonction « Permissions » dans Outlook pour déléguer quelqu'un qui pourra agir à votre place. Il ne faut PAS acheminer le courrier électronique vers une adresse INTERNET parce qu'il peut contenir des renseignements de niveau Protégé A et qu'Internet n'est pas une zone protégée.

Utilisation des disquettes

Enregistrez vos fichiers de données sur des disquettes à code de couleur approuvées, et collez sur chacune une étiquette indiquant le niveau de classification ou de protection approprié. Les codes de couleur pour les disquettes sont les suivants.

Code de couleurs des disquettes

COULEUR	SYSTÈME À UTILISER	NIVEAU DE CLASSIFICATION OU DE PROTECTION AUTORISÉ
Jaune	Système accrédité pour traiter les renseignements Très Secret	Très Secret
Rouge	SIGNET C4	Secret, Confidentiel, Protégé B et C
Toutes les autres couleurs	SIGNET 2000+ SIGNET 3	Protégé A et Non Classifié

Même si la couleur de la disquette indique « en principe » le niveau de sécurité des renseignements qu'elle contient, une étiquette indiquant le niveau de classification LE PLUS ÉLEVÉ des renseignements devrait également être collée sur la disquette.

Élimination ou réutilisation des disquettes et du matériel

Si les disquettes, les disques durs ou les ordinateurs portatifs spécialisés contiennent des renseignements du niveau Protégé B jusqu'au niveau Très Secret, envoyez-les à SPAS avec la mention « pour élimination ». Si les disquettes, les disques durs ou les ordinateurs portatifs doivent être réutilisés dans le même milieu (traitement de documents du niveau Protégé B au niveau Secret), communiquez avec SXTC pour leur nettoyage.

Si les disquettes ou les disques durs contiennent des renseignements non classifiés ou de niveau Protégé A, communiquez avec les services de soutien SIGNET pour que leur contenu soit supprimé en toute sécurité avant qu'ils soient réutilisés ou jetés.

Protéger son système contre les virus

Les logiciels de détection de virus d'AEC et de CICan enlèvent automatiquement les fichiers exécutables qui sont joints à des courriers électroniques destinés à des correspondans de l'extérieur du Ministère ou provenant de correspondants de l'extérieur. Ainsi, si vous recevez un courrier auquel était joint un fichier exécutable, vous recevrez un message du logicial Antigen vous indiquant que le fichier joint a été enlevé.

Si vous certifiez que le fichier est essentiel aux activités du Ministère et respecte les politiques d'utilisation acceptable, vous pouvez vous faire envoyer ce fichier en faisant parvenir le courrier automatisé à -EXTOTT -SXIM -OPS et en fournissant les attestations requises.

Lignes directrices

- Assurez-vous de toujours effectuer une vérification en vue de détecter des virus.
- Utilisez toujours le logiciel de détection de virus installé sur le réseau pour vérifier chaque disquette provenant d'un autre poste de travail avant de vous en servir.
- Si vous recevez un message indiquant la présence d'un virus dans votre poste de travail, communiquez avec les services de soutien SIGNET ou avec votre administrateur de système. N'arrêtez pas le système et ne tentez pas de supprimer vous-même le virus.

Si vous détectez un virus ou en soupçonnez la présence, communiquez immédiatement avec votre administrateur de système.

Utilisation du réseau d'AEC et de CICan

La politique relative à l'utilisation des réseaux électroniques d'AEC et CICan s'applique à tous les employés (ceux du gouvernement fédéral, les fournisseurs, etc.) qui ont un accès autorisé aux réseaux du Ministère ou à INTERNET au moyen des ordinateurs, des réseaux d'interconnexion ou des ordinateurs autonomes munis de modems d'AEC et CICan. Pour plus amples renseignements, veuillez consulter le document suivant : http//intranet.lbp/department/sxd/policy/policy-f.asp

Il revient à chaque utilisateur du réseau d'AEC et CICan d'en faire usage à des fins autorisées et d'une manière légale et acceptable. Les utilisateurs de SIGNET 2000+/SIGNET 3 qui abusent des privilèges qui leur sont accordés, par exemple pour le courrier personnel et l'utilisation d'INTERNET, peuvent se les voir retirer. Si les abus persistent, des mesures disciplinaires ou de courrection pourraient être prises.

Utilisation d'Internet

Le Ministère a publié une série de lignes directrices à suivre lorsque vous utilisez Internet. Vous les trouverez sur l'INTRANET du Ministère sous la rubrique Politique sur l'utilisation des réseaux électroniques (PURE). Pour de plus amples renseignements ayant trait à la PURE, veuillez consulter le site Web suivant : http://intranet/policy-f.htm

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 dans 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.

Nota : AEC et CICan surveillent l'utilisation d'Internet et du courrier électronique. Les abus peuvent entraîner des mesures disciplinaires.

Conseils pour l'utilisation responsable d'Internet

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 dans un site provoque la création d'un fichier témoin qui peut permettre de remonter jusqu'à vous à des fins de commercialisation et de facturation.
- ❑ N'oubliez pas non plus que AEC et CICan surveillent 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 à ce sujet, appelez l'InfoCentre (944-1776).
- ❑ Protégez la sécurité et l'intégrité de SIGNET 2000+ en vous assurant qu'il n'y a aucun virus dans les documents que vous téléchargez d'Internet.
- ❑ Utilisez seulement des logiciels commerciaux approuvés pour Internet.
- ❑ Connaissez les sources autorisées pour les réparations, l'entretien, les mises à niveau, etc.

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 comme le piratage informatique ou la pornographie juvénile.
- ❑ 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.
- ❑ Donner un accès non autorisé à votre accès à distance à des amis ou des membres de votre famille.
- ❑ 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.

PROCÉDURES À SUIVRE LORSQU'ON QUITTE SON EMPLOI À AEC ET CICan

Peu importe les circonstances dans lesquelles vous quittez votre emploi, il importe de comprendre et respecter vos obligations en matière de sécurité. Au moment de votre départ du Ministère, vous devez vider vos classeurs et autres meubles de rangement, et vous assurer qu'aucun document, disquette ou autre matériel ne soit enlevé ou éliminé d'une manière irrégulière.

Tous les documents doivent être supprimés conformément à la Politique des archives nationales et aux exigences ministérielles en matière de sécurité.

Vous devez aussi :

- Remettre à votre superviseur tous les documents qui contiennent des renseignements classifiés ou protégés, ainsi que tous les biens et renseignements gouvernementaux que vous avez obtenus durant votre période de service.

- Rendre votre carte d'identité à la Section de l'identité (pièce BG-180)..

- Remplir le formulaire TBS-SCT 330-25 : Annulation de la vérification de fiabilité/Autorisation de sécurité pour des raisons administratives.

- Rendre vos clés de bureaux à l'adjointe administrative ou à la personne responsable des clés dans votre section.

SECURITY AND SAFETY PRACTICES AT DFAIT FACILITIES IN CANADA

DEPARTMENT OF FOREIGN AFFAIRS AND INTERNATIONAL TRADE CANADA

ISC - October 2006

IMPORTANT TELEPHONE NUMBERS	
Need a new key, combination padlock or new padlock? Locked out of your office?	Send E-Mail to SPAS 992-6678 (SPAS Lockshop)
Need information on disposing of classified and protected information?	992-6680 (SPAS)
Need an ID Card/building pass or temporary pass?	(SPAS - ID Section) 992-6691 (LBP - BG-180)
Need passport or visa photos?	(SERV/ID Section) 944-3074
Lost something?	944-0019 (SPAS)
Want to know about courses, seminars, briefings, or job aids on security?	992-6704 (ISC)
You have questions on the security screening process?	992-6703, 992-6706, 992-3471, 992-1905 or 944-1889 (ISCT)

EMERGENCY TELEPHONE NUMBERS	
Ambulance	8+911
Ottawa Police Services	8+911
Ottawa Fire Department	8+911
LBP First Aid Station	992-1150
LBP Fire/Safety Control Centre	992-1150
LBP Commissionaires (Security Office)	992-5452
LBP Chief Building Emergency Officer	992-5218
LBP Deputy Chief Building Emergency Officer	992-6680
Public Works and Government Services Canada Building Engineer	1-800-463-1850
111 Sussex First Aid Station	944-2887
111 Sussex Fire/Safety Control Centre	944-5555
111 Sussex Commissionaires (Security Office)	944-5551
111 Sussex Chief Building Emergency Officer	992-5452
111 Sussex Deputy Chief Building Emergency Officer	944-2597
111 Sussex Property Management (BLJC)	8+241-8192
Poison Control Centre	8-737-1100
Labour Affairs Officer - Human Resources Canada	946-2800

TABLE OF CONTENTS

ABOUT THIS DOCUMENT

This handbook will help you perform your security responsibilities as a new employee of the Department of Foreign Affairs and International Trade (DFAIT).

Security is an important factor in your day-to-day decisions – from the identification, handling, storage, transmission, and proper destruction of classified and protected information to the use of secure equipment and access to restricted zones. 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.

Most aspects of both the physical security and the emergency procedures provisions described in this handbook apply specifically to the Lester B. Pearson (LBP) Building and 111 Sussex Drive (former City Hall) 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 local security and emergency arrangements.

Since most of the information in this handbook pertains to the Lester B. Pearson (LBP) Building and 111 Sussex Drive, it is not intended to replace 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 Headquarters Security Operations Section (SPAS).

If the handbook doesn't answer all of your questions, ISC offers courses and briefings that are scheduled on a regular basis. Contact the Security Education and Awareness Program (ISC) at 992-6704 for its *Calendar of Courses*.

INTRODUCTION

The Department of Foreign Affairs and International Trade (DFAIT) is 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. This information must be safeguarded.

The Department also holds valuable assets. DFAIT owns and leases chanceries or official residences, staff quarters, vehicles, works of art and office equipment 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 is concerned for the safety of its employees and their dependants who live and work abroad in widely varying environments. Many of these environments are more dangerous than that in Ottawa. This concern is a principal feature distinguishing the security policy of DFAIT from that of other Canadian departments and agencies which focus on security of information issues.

Good common sense and an ounce of prevention are often all that is required to ensure your safety and the safeguarding of information and assets.

SECURITY MEASURES AT HQ

The Headquarters Security Operations Section (SPAS) develops and implements all procedures, orders and instructions for any situation that may affect either the safety of personnel or the safeguarding of government assets including information at HQ.

Building Emergency Procedures

Simple emergency procedures for the LBP Building and 111 Sussex* are available in the *Manual of Security Instructions* and in the booklet *Emergency Procedures - Employee Handbook.* These procedures 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.

Please take the time to read the Emergency Procedures - Employee Handbook located at the entrance of every tower. It also can be found on the DFAIT Security website:
http://intranet/dfait-maeci.gc.ca/department/security/guides/emergproc-e.asp

* NOTE: Separate Emergency Procedures are in effect for 111 Sussex.

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 your responsibility to safeguard 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 SPAS (Security Operations) at 944-0019. If government property is either lost or stolen, also report it to SRAA (Headquarters Facilities Management Section) at 996-6816 and to SMSP (Financial Planning and Reporting) at 944-1102.

Physical Security at HQ

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

- daily monitoring of the flow of people into restricted zones;
- 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.

Zones

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

Public Zone
This zone surrounds or forms part of the facility. Examples include cafeterias, banks and lobbies.

Reception Zone
Located at the entrance to the building, this zone is defined as 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 is the Services Centre (SERV) in the LBP Building.

Operations Zone
Access to this zone is limited to personnel and to visitors who are escorted by employees with a valid security clearance. This includes all the towers and pavilions.

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

Accessing a Zone - Building Passes

Swipe card entry devices are installed at the entrance of each tower of the LBP Building and at various locations at 111 Sussex. All employees must visibly display their building pass at all times while in these buildings and other departmental facilities. The following colours of departmental photo ID passes allow access to the LBP Building and 111 Sussex.

Blue Pass
The Blue pass is issued to personnel who have at least a Level II (Secret) security clearance and allows access to the controlled areas 24 hours a day, 7 days a week. The Blue pass also allows The employee to escort visitors displaying a Red Visitor's Pass or employees who do not have a building pass to restricted access areas of the Department.

Green Pass
The Green pass is issued to personnel such as term employees or contractors, who have at least a Level II (Secret) security clearance and allows access to the controlled areas unescorted during core hours only - 0700 to 1800 hours, Monday to Friday, regular business days. You cannot escort visitors or others into the controlled areas with this pass.

Red Pass
The Red pass is issued to non-governmental personnel who provide services to DFAIT and do not require access to restricted areas. Red pass cardholders do not possess a security clearance and must be escorted in controlled areas.

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

Pink Pass
The Pink pass is issued to personnel who have a Reliability Status (formerly referred to as an ERC). The temporary pass is for new employees awaiting a security clearance and for those hired for short-term contracts, including summer students.

It allows access only to the controlled areas of a specific facility (LBP or 111 Sussex etc.) Pink pass holders are subject to the following conditions:

- your access is restricted to a period not exceeding six (6) months;
- you have no access to classified information, although you can access Protected A material;
- you must at all times be supervised by a security-cleared employee;
- you cannot escort others into the controlled areas.

The Pink Building Access Card is provided by SPAS following the authorization of a Reliability Status by ISCT.

Maroon Pass

Issued on a reciprocal basis to certain other specific countries. This pass has the same access levels and conditions as the Green Pass. Should you require further information on this contact SPAS.

Blue/Green Contractor "C" Passes (with photo)

Issued to services provider contractors who repeatedly respond to DFAIT - HQ for the purpose of servicing equipment and systems within. Such persons are security cleared. Passes are similar in appearance to a departmental employee pass except the company name appears above a large "C" to the left of the bearers photograph. The card colour depicts the access privileges of the bearing.

Temporary Yellow "C" Pass

Issued to security cleared contractors who are carrying out work within DFAIT - HQ during a very limited time frame. The brief period of stay does not justify the issuance of a Contractor "C" Pass with photograph.

NB - With respect to the other DFAIT offices within the NCA, the presence of Contractor "C" Passes with photo is probable as often a service provider responds to specific client needs regardless of venue.

Where a difference may be noted is in the appearance of the *Temporary Contractor Pass* issued by the responsible building management/assigned guard force. Clarification may be requested by contacting the building management of the respective site.

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.

Protect the security of our department and the safety of the workplace by challenging any person without a pass who may be coming in when you use your card to enter, or when you exit the doors to any of the towers. SPAS (992-5452) should be called immediately if you encounter any problems.

To Obtain a Building Pass

Building passes are issued by SPAS at the SPAS Identification Section which is located in Room BG-180 (7:00 a.m. to 2:45 p.m.). A building pass can only be authorized after verification of a reliability status or security clearance. Please note that temporary passes and fingerprinting are only available in the SPAS Identification Section, Room BG-180.

To Obtain Diplomatic Passports and Visas

Photographs for diplomatic passports and visas will be processed during the same operational hours in the Services Centre (SERV), Room D1-423 of the LBP Building, telephone 944-3074. For questions regarding official passport eligibility, details, visa details, time of processing, etc. please contact JWC at 944-3550 (tel) or 997-1255 (fax).

A Posting Confirmation Form or Travel Authority is required prior to providing photos. For special needs please forward an e-mail to Ann Séguin-Huskas (SPAS).

Visitor Passes

A visitor pass will be provided only in exchange for a valid piece of photo identification for all persons who are not in possession of a valid DFAIT identification card. Visitor passes must be visibly worn for the duration of the visit. There are two types of visitor passes:

Yellow Visitor Pass

Issued to visitors whose security clearance, Secret at a minimum, has been confirmed by SPAS and are registered as such in the VPIS. Visitors issued with a yellow visitor pass do not require to be escorted while on the premises. Guards will notify the host employee when their guests have arrived.

Red Visitor Pass

Issued to visitors whose security clearance has not been ascertained. Visitors issued with a red visitor pass must be escorted at all times while in the building. Guards will notify the host employee when their guests have arrived. Once the visit is confirmed, Commissionaires will escort visitors to their destination. Departmental personnel will be responsible for ensuring that visitors are escorted back to the Main Lobby upon their departure.

The current practice of pre-registering visitors will continue to be available by contacting the Main Reception by e-mail at DFAIT Front Desk/Réception MAECI - SPAS and providing information on meeting particulars and attendees.

Visitor Access

Visitors to restricted areas must be escorted at all times. 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 LBP Building or 111 Sussex.

Reception Desk Services at HQ

The DFAIT reception desk staff can receive your guests or visitors more quickly and efficiently through your Profiles data in the Staff Profiles application. Staff also depend on being able to reach you by telephone when visitors arrive.

Please ensure that your profile data, such as your office number and telephone number, is up to date by going to CorpApps Profile Database. For more instruction please use the following link: http://intranet.lbp/department/sxd/howTo/genpro-e.asp

Please advise SPAS of any visitors you are expecting. You can do this in one of three ways:

1. E-mail: DFAIT Front Desk / Reception AEC et de CICan - SPAS (reception@FACITCan-acccican.gc.ca)
2. Voice mail: 995-5859
3. Visit the front desk and provide a paper copy with names of expected guests.

Access to Controlled 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 advisable to register in and out of the buildings during quiet hours. This record will indicate who is in the building and where personnel are located in case of an emergency.

The Alarm System During Quiet Hours

Access control doors located at the entrance to the towers and the pavilions 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.

Parking

Parking permits are issued by the Headquarters Administrative Services Division (SPAA) located on the main level of Tower D in the LBP Building. If you have any questions about these permits, contact SPAA (992-2338). SPAS, through a special arrangement with the RCMP, enforces the parking regulations established by the Government Property Traffic Regulations.

Responsibilities of the Canadian Corps of Commissionaires

The Canadian Corps of Commissionaires provides security guard services in the LBP Building and 111 Sussex. They may request the presentation of ID cards. Commissionaires are responsible for:

- controlling reception and access;
- monitoring and responding to the building alarms systems;
- conducting security and fire patrols;
- controlling and escorting visitors to an employee's office after contacting that employee;
- monitoring the movement of material in/out of the LBP Building and 111 Sussex.

IDENTIFYING AND SAFEGUARDING INFORMATION

The Government Security Policy establishes policy guidelines for information security and privacy requirements. DFAIT must properly safeguard personal information and other sensitive data in its information systems or used in its programs and services. Safeguards for information and assets should clearly reflect their sensitivity, importance and value - no more and no less.

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

There are three levels of security grading for the purposes of safeguarding information:
- Unclassified
- Protected
- Classified

In your day-to-day work, make sure that you can identify information that requires safeguarding, and mark information correctly using the appropriate security marking. For example, Secret, Protected A, etc., so that others see the need for special safeguarding.

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.

Identifying Classified and Protected Information

Not all information needs to be classified or protected. Some information and certain assets are more sensitive or valuable than others and, therefore, require stricter safeguards. In line with the provisions of the *Access to Information Act, the Privacy Act* and the *Government Security Policy* you are to identify the security grading for the information you create.

At a minimum, departmental information and assets should receive a level of care that is consistent with basic administrative practices. Certainly, information should never be classified nor protected to conceal violations of the law, inefficiencies or administrative errors, nor to avoid embarrassment or to restrain competition.

Classified Information

Information is classified if its unauthorized disclosure could injure the national interest of Canada, that is, the defence and maintenance of the social, political, and economic stability of the country.

Classified information has three levels:

1. **Top Secret** - when compromise of the information could reasonably be expected to cause **exceptionally grave injury** to the national interest, for example:
   - potential armed hostilities toward Canada or its allies
   - information about intelligence services
   - reports which could result in the death or torture of an individual

2. **Secret** - when compromise of the information could reasonably be expected to cause **serious injury** to the national interest, for example:
   - records of discussions of Cabinet or Cabinet committees
   - details of important international negotiations
   - developments relating to federal-provincial or national security

3. **Confidential** - when compromise of the information could reasonably be expected to cause **injury** to the national interest, for example:
   - record of discussions of interdepartmental committees
   - instructions on safeguarding highly classified information
   - reports from missions that might affect international relations

Protected Information

Information is protected if its compromise could cause injury to private and other non-national interests for which the government has an obligation. The information requires safeguarding, but it does not affect the national interest. The three levels of protected information are:

1. **Protected C** - when compromise of the information could reasonably be expected to cause **a high degree of injury** to private and other non-national interests such as to the safety of individuals; for example, important commercial information, law enforcement.

2. **Protected B** - when compromise of the information could reasonably be expected to cause a **medium degree of injury** to private and other non-national interests. Serious injury includes lasting harm or embarrassment that will have negative effects on an individual's career, reputation, etc.; for example, solicitor-client privilege, company financial information, personnel appraisals.

3. **Protected A** - when compromise of the information could reasonably be expected to cause **a low degree of injury** to private and other non-national interests; for example, disclosure of an individual's exact salary, Social Insurance Number.

Information from Other Organizations

Information received from any level of government in Canada, from governments of other nations, or from international organizations, must be safeguarded at the level as defined by that organization. For example, if you are preparing a briefing note for a document classified as SECRET, you simply classify the briefing note as SECRET.

The Classification and Protection Guide explains how you should mark the following:	
• bibliographies and sources • third-party information • file folders • forms	• NATO documents • documents for external use • documents with caveats

For more information, please see our web site: http://intranet/dfait-maeci.gc.ca/ department/ security/menu-e.asp.

Automatic Declassification or Downgrading

Information must be classified/protected for the time it requires safeguarding only. Once that time has passed, the classification/protection label should be removed or downgraded. When you create a document you can specify a date or event after which the document can be declassified or downgraded. For example:

- Confidential (Unclassified after 31 July 2002)
- Protected A (Unclassified if Annex A removed)

Changing a Document's Level of Classification or Protection

If you want to change the level of classification or protection of a document, you must:

- be the originator or an employee who replaced the originator;
- have clear proprietary responsibility for the information; or,
- have a detailed knowledge and familiarity of the sensitivity of the information.

The date, authority and the new level of classification/protection should be clearly marked in ink on the top right-hand corner of the document.

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

If a security grading 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 Privacy Protection Division (DCP).

Handling Classified and Protected Material

Many documents move in and out of the Department. Since some are more sensitive than others, special handling procedures need to be followed. For detailed information, see the appendices (located at the entrance of the towers and pavilions) referred to in the following table.

Transmittal Standard (See Appendix A)	***Transport Standard*** (See Appendix B)
The transfer of classified or protected information or assets by someone without a "need-to-know" the information.	The hand-carried transfer of classified or protected information or assets by any Departmental employee with an appropriate clearance (reliability status or security clearance and a "need-to-know" the information.

Secure Telephones and Facsimiles

A secure telephone, known as a STU-III, provides a secure telephone capability for all personnel who need to discuss or transmit classified and protected information. The terminal may be used as an ordinary telephone, completely inter-operable 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.

Note: The terminal on its own is UNCLASSIFIED. The Cryptographic Ignition Key (CIK) on its own is also UNCLASSIFIED. However, when the CIK is inserted inside the terminal, the item then becomes CLASSIFIED.

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

- when a STU-III terminal or a CIK is lost or stolen;
- when a CIK has been left in the terminal unattended; or
- when a STU-III appears to be tampered with.

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.

Under certain conditions, you may be authorized to receive/listen to classified/protected information over the STU-III while you would only be authorized to speak at an unclassified level.

Storing Classified and Protected Material

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

DFAIT Headquarters receives over 40,000 visitors annually, so if you are away from your office for an extended period of time, lock your door, if you are in an open area, store classified and protected material in a secure place.

Discussing Classified and Protected Information

- Classified and Protected C information should not be discussed in open areas nor on open or unsecured telephone lines.

- When you discuss classified and protected information with someone, ensure that the person is informed of the information's security grading, and that the person has the appropriate access level.

- In the case of a lecture or other public event, the audience should be reminded, both at the beginning and end of the event, that the intended information may be classified or protected, and at what level.

Minimum Storage Requirements for Classified and Protected Material

The minimum requirements for storing classified and protected 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 operations zone in a security file cabinet with double hasp and approved combination padlock.

Changing a Combination Lock Setting

Combination settings should be changed:
- when the person knowing the combination is transferred, terminated, or no longer requires access to the information;
- when a new person is hired; or
- when the combination is or may have been compromised;

Please forward your request by e-mail to SPAS.

Office Keys

The Administrative Assistant 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, ask the Administrative Assistant or person responsible for keys in your Section to unlock the door. If neither person is available, telephone the SPAS Lockshop at 992-6678 to have the door unlocked. The SPAS Lockshop will do so, but the response time will depend upon the availability of personnel.

- Safeguard your keys at all times
- Do not copy keys; spare keys are to be controlled by the Administrative Assistant or a designated person
- New keys may be obtained by the Administrative Assistant e-mailing the request to the SPAS Lockshop.

Failure to adequately safeguard keys is a SECURITY INFRACTION.

Use of Absent Cards

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

If you know you will be away, contact SPPM to obtain an absent card to be placed on the top of your desk. Do not leave any classified/protected documents or materials on your desk.

Working on Classified and Protected Material at Home

Sometimes you may need to work with classified/protected material during the evenings or on the weekend, but the practice of taking classified/protected information home or any other place is not recommended. 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; and
- you must safeguard the information at all times.

Equipment and material (including computer equipment and software) cannot be removed from DFAIT without a completed GC205 *"Authority for Removal of Material from Premises"* form. Likewise, use form CG 205 to remove personal belongings that may appear to be government property.

Disposing of Classified and Protected Information

Classified (Confidential and Secret) and Protected (Protected A, B and C) documents must be disposed of by using the shredders located on all floors. If you have a large volume of classified waste (for example, if your Division is relocating or wishes to dispose of Top Secret documents), please forward an email to SPAS to arrange for pick-up or for guidance. Unclassified information should be recycled.

Security Incidents (Breaches and Violations)

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

If a security incident 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 protect information according to the Government Security Policy;
- classified or protect information in contravention of the Government Security Policy;
- altered, kept, disclosed or removed classified or protected information or assets without authorization;
- failed to safeguard classified or protected information or assets; or
- processed classified or protected information above Protected A on SIGNET 3.

Commissionaires are authorized to conduct periodic security checks. If they notice unsecured cabinets, classified and protected documents left exposed without adequate safeguarding, or combinations or keys for security containers left in open desks, they are required to issue Security Infraction Notices. These violations will also be reported to ISC.

When unsecured material is found, it can be impounded and held by SPAS. The 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 SPAS when you retrieve the confiscated material.

Tips for Safeguarding Classified and Protected Material

- Adopt a clean desk policy; during the day, place classified and protected material on your desk only, not on cabinets, windowsills or in desk drawers.
- At the end of each day do a visual check of your office.
- Always assume that when you leave for a meeting you will not be returning, and store all classified and protected material in your cabinet.
- Leave an Absent Card on your desk.
- Always lock your office when leaving for the day or for a meeting.

Sanctions for Breaching or Violating Security

The Deputy Minister has the right to apply administrative and/or disciplinary sanctions if breaches and violations occur. Sanctions may include:

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

Handling Cabinet Documents

Cabinet documents are circulated by hand to Ministers, the Deputy Minister and to Departmental employees who 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 Cabinet and Parliamentary Affairs Division (DCL). DCL also maintains a bring-forward system and reminds officers when the document is nearing its return date.

Privy Council regulations require that all Cabinet documents provided for Departmental use be returned to DCL within a set period of time, especially with the end of regular, weekly Cabinet meetings at the end of a session.

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

If divisions require these documents for use, for example, during the summer period, arrangements can be made to redistribute documents that have been returned to DCL.

PERSONNEL SECURITY SCREENING

Access to Government Assets (including information)

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

All departmental employees must undergo a security screening process before being appointed to their position.

There are two types of security checks:

- the Reliability Check (RC)
- the Security Assessment

To have access to Government assets including information, you MUST have a valid Reliability Status.

The Reliability Status (RS)

Prior to the appointment of an individual to a position, a Reliability Check must be done and a Reliability Status granted. An individual granted a Reliability Status may have access to unclassified and protected information and assets.

Verification and validation of the following checks are required:

- ❑ personal and employment data
- ❑ educational and professional qualifications
- ❑ accreditations or certifications
- ❑ references
- ❑ criminal records
- ❑ credit rating
- ❑ name indices check (vetting), if required

Once the RS has been authorised, access is granted on a need-to-know basis to protected information (Protected A, B and C).

Procedures for Conducting a Reliability Check (Prerequisite to a Security Clearance)

Before appointing a new employee, the responsible manager or staffing officer is required to submit by mail or by hand the following forms to conduct the Reliability Check.

Forms Required
❑ Personnel Screening Consent and Authorization Form (TBS/SCT 330-23) ❑ Security Clearance Form (TBS/SCT 330-60) - for all clearances. ❑ A set of fingerprints taken by SPAS ID room (only for Top Secret clearances or if requested by ISCT). *All forms, other than the fingerprint form, are available on the Intranet Services, Forms on line.*

Procedures for Completing the Personnel Screening Consent and Authorization Form TBS/SCT 330-23

1. At the top of the form indicate whether this is a new request or an upgrade to a higher level. Also indicate that the request is for a Reliability Check.

2. **Part A:** The individual to be screened must complete and ensure that all given and family names (including maiden and patronymic and matronymic names, and any legal name change, if applicable) are provided. This is most important as the Criminal Records Name Check is to be undertaken using all names.

3. **Part B:** "Particulars of Appointment". Complete and provide all information with respect to the position itself. Insert the name and address of the "Originator of the Request" as well as telephone and facsimile numbers.

4. **Part C:** "Screening Assessment and Consent". Have individual sign, date and initial boxes 1 through 4. Request confirmation of Reliability Status with ISCT.

5. Ensure that the individual to be screened provides the following:
   - consent to the disclosure and subsequent verification of the information, by initialing all boxes
   - written consent, by signing and dating the consent portion of the form, Part C.

6. Once the individual has given consent to the verifications, proceed as follows:

Process of Verification Used in Reliability Checks (Part C, Box 1)

To be verified by the hiring manager or the staffing officer:

1. Proof of Identity (Personal Data)
   Part C, (Physical check of documents, i.e. birth certificate, passport and photograph)
   To prevent impersonation; to ensure that the records checked are those of the individual being checked.

2. Educational Qualifications
   Part C, (Physical examination of degrees, certificates and contact with the educational institutions)
   To ensure that the individual is being truthful about background and history. To verify the period of education and the degree attained and that the institution is a bona fide educational institution as opposed to a diploma mail-order business.

3. Employment History (5 year)
   Part C, (Telephone calls to previous employers is sufficient)
   To determine reliability in previous employment and to ensure that the person is being truthful about background and history. It is suggested that you cover a five year period. If the individual has had six jobs in the last five years, call all six employers.

4. References (5 year)
   Part C, (Completed at the same time as the verification of employment history)
   To determine whether the individual has been honest, trustworthy and reliable. References should be questioned about their knowledge of the individual and about the background and character of the individual.

To be completed by ISCT

5. Criminal Record Check
   Part C, Box 2
   To determine whether the individual has in the past committed crimes that would indicate unacceptable risk in relation to the duties to be performed. Factors to be considered are whether the individual was a one-time or repeat offender, whether the crimes were committed recently or long ago and how the crime(s) relates to the job requirements.

6. Credit Check
   Part C, Box 3
   To determine whether the individual might be subject to financial pressures that could reflect on the degree of trust required in relation to the duties to be performed. This is especially important if the employee is to handle funds, financial databases, or land/property acquisitions and the purchase of supplies.

7. CSIS Loyalty
   Part C, Box 4

8. CSIS Name Indices Check (Vetting)
Part C, Box 5
To determine whether there are national security reasons for denying an applicant employment.

Box 5 is used only where prior to Treasury Board of Canada Secretariat approval has been obtained.

According to the GSP: access to classified information and assets is limited to those individuals who have undergone a security assessment and are granted a security clearance at the appropriate level. HE OR SHE MUST NOT be appointed to a position requiring access to Classified information and assets until the security clearance has been granted.

The Security Clearance

A security clearance is required for anyone who has access to classified information or assets, regardless of the type of employment. This security assessment process is completed in addition to the 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.

Three levels of security clearances, which correspond to the three levels for classified material:	
Level I	Access up to CONFIDENTIAL
Level II	Access up to SECRET
Level III	Access up to TOP SECRET

A Level II - SECRET clearance is generally required for employment at HQ.

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

Marriage or Cohabitation

If you have a valid security clearance and plan to marry or cohabit (including a same-sex relationship), you must complete Form EXT 332 Intent to Marry or Cohabit and submit it to ISCT for security verification. Based on the information you provide, a security assessment will be carried out on the intended spouse to find out whether anything is known about him or her that would indicate if you, the employee, might act against the national interest.

Personal Behaviour

Most personal matters are not of security interest to the Department. However, some activities, especially when serving abroad, could result in a person being threatened or blackmailed in such a way as to be a threat to the security of Canada, or a threat to the safeguarding of information classified in the national interest.

Examples of the kind of activity in question include:

- alcohol abuse;
- mismanagement of personal finances;
- non-medical use of narcotics;
- personal problems which could affect security clearance; or
- suspicious contacts with foreign nationals and criminal organizations.

All employees should be familiar with, and adhere to, the Department's *Code of Conduct*, which may be viewed at:

http://intranet.dfait-maeci.gc.ca/department/SPD/HRmanual/echap2.htm

Downgrading/Revocation of Reliability Status or Security Clearance

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

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

The authority to review, revoke or suspend a Reliability Status rests with the delegated manager.

In both instances, the individual is advised of the right of review or redress and prohibited from access to classified and/or protected information and assets.

SECURITY OF INFORMATION TECHNOLOGY (IT)

IT Security ensures the safeguarding of departmental systems, assets, information, and services against deliberate and accidental threats to:

- Confidentiality of information;
- Integrity of processes and data; and,
- Availability to data, systems and services

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

IT also includes all the data and information you create while carrying out your job function; your official reports, memos, e-mail messages, etc., are government records and belong to the Crown.

Why IT Security is Necessary

As DFAIT employees, there are a number of threats to IT security against which we must safeguard ourselves.

- *Deliberate* threats which include: unauthorized access to departmental data, electronic eavesdropping, non-compliance with DFAIT practices, and viruses.
- *Accidental* actions or events which include: user errors, lack of user knowledge, breakdown of computer hardware.

Departmental Networks

The systems we use to process information comprise the following departmental networks:

- SIGNET 3 (formerly known as SIGNET-D); and
- SIGNET C4.

SIGNET 3

The main departmental network used for processing unclassified and Protected A information at headquarters and missions is SIGNET 2000+/SIGNET 3. This system is accessible to all employees including locally-engaged staff abroad. It is also available to a few other government departments, organizations and some foreign governments. In the majority of missions, the SIGNET 2000+ system is administered by a locally-engaged system administrator.

Note: Personnel must have, at minimum, a Reliability Status (RS) before obtaining access to SIGNET 2000+/SIGNET 3.

Working With Classified and Protected Data

You need to know what IT equipment you can use for different levels of protected or classified information. There are two principles to keep in mind:

1) Departmental IT systems are approved to process information up to a specified maximum level of security. Applied security measures provide a level of safeguarding appropriate for information up to that specified level.

2) The level of sensitivity of the information dictates the IT equipment or IT system you must use.

The general rule is: select an IT system with adequate security measures for the sensitivity of your information. If you are to be working with IT for Protected B to Secret information, use SIGNET C4.

SIGNET C4

SIGNET C4 is distinct and separate from SIGNET 2000+. Access to this network is available to employees who possess a minimum Level II (Secret) clearance and who have a need to process and transmit information classified up to SECRET. Because SIGNET C4 is used for more sensitive information, it has additional security features such as:

- a removable hard drive that can be stored when unattended; and
- approved encryption.

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 and procedures.

Tips for Network Use

- Include a classification/protection label on all messages that are printed, stored or transmitted.
- Log off your work station (SIGNET 2000+ and C4) when you leave it unattended.
- Use approved software on servers and work stations.
- Do not install modems or connections to other computers or networks, unless authorized to do so by the system owner.

Your Password

Your password is you. It is the security measure that protects YOU and YOUR IDENTITY, and it is DFAIT's security measure preventing unauthorized access to our systems. Never reveal your password to anyone — remember, anyone using your password can masquerade as you, resulting in serious implications for your career, as well as for DFAIT security.

When you are absent, use the auto-forward option to forward your e-mail to a colleague; or, use the "Permissions" tab in Outlook to delegate someone to act on your behalf. Do NOT forward your e-mail to an INTERNET address because some e-mail received may contain protected or classified information and the Internet is not secure.

Using Diskettes

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

Diskette Colour Codes

COLOUR	SYSTEM TO BE USED	APPROVED LEVELS OF CLASSIFICATION OR PROTECTION
Yellow	System accredited to process Top Secret information	Top Secret
Red	SIGNET C4	Secret, Confidential, Protected B and C
All other colours	SIGNET 2000+/SIGNET 3	Protected A and Unclassified

Even though the diskette colour "technically" identifies the security grading of the information it contains, the diskette should also be labelled according to the HIGHEST classification of the level of information it contains.

Disposal and/or Reuse of Diskettes and Equipment

If diskettes, hard drives and dedicated laptops contain Protected B to Secret information, send them to SPAS marked "for destruction". If diskettes, hard drives or laptops are to be reused in the same environment (for processing Protected B to Secret), contact SXTC for sanitization.

If diskettes or hard drives contain unclassified or Protected A information, contact SIGNET Support to have the media securely deleted before reuse or disposal.

Safeguard Your System from Viruses

DFAIT's anti-virus software products automatically strip executable attachments on e-mails to and from correspondents external to the Department. Thus, if you receive or send a message containing a stripped e-mail attachment, you will receive a message from the Antigen anti-virus software saying the attachment was removed.

If you certify that the file is essential to the business of the Department and respects acceptable use policies, you may arrange for its delivery by forwarding the automated e-mail to -EXTOTT - SXIM – OPS, providing the required certifications.

Guidelines

- Make sure you scan for viruses.
- Always use the anti-virus software installed on the network to scan each diskette coming from another workstation before you use it.
- If you get a message reporting a virus on your machine, contact SIGNET support or your System Administrator. Do not shut down your system or try to remove the virus yourself.

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

Use of DFAIT Networks

The policy governing the use of DFAIT electronic networks applies to employees (federal, contractors, etc.) who have authorized access to the Department's electronic networks or to the INTERNET through use of the Department's computers, network connectivity or stand-alone workstations via modems. For more information please use the following link:
http://intranet.lbp/department/sxd/policy/policy-e.asp

Any user of a DFAIT network is responsible for ensuring that he or she uses the network for authorized purposes only and in a lawful and acceptable manner. Privileges granted to users of SIGNET 2000+/SIGNET 3, for example, for limited personal use of e-mail and access to the INTERNET, can be revoked if abused. Continued abuse may lead to additional disciplinary or other remedial actions.

Use of the Internet

The Department has issued a set of guidelines to be followed when using the Internet. These are available on the departmental INTRANET site under the *Network Acceptable Use Policy* (NAUP). Personnel interested in knowing more about the NAUP may view the information following this web site address: http://intranet/policy-e.htm

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.

Note: DFAIT monitors Internet traffic and e-mail traffic uses. Any abuse may lead to disciplinary measures.

Tips for Responsible Use of the Internet

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 Info Centre (944-1776).
- ❑ Protect the safety and integrity of SIGNET 2000+/SIGNET 3 by checking for viruses on anything you import from the Internet.
- ❑ Use only approved commercial software programs for Internet use.
- ❑ Know which authorized sources to call for repairs, maintenance, upgrades, etc.

Do not

- ❑ use for personal gain.
- ❑ use for commercial activities (for example, the unsolicited distribution of advertising material).
- ❑ use for unlawful or malicious activities such as hacking or child pornography.
- ❑ 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.
- ❑ provide unauthorised access of your remote access to users such as friends or family.
- ❑ upload 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-in into any computer or system, whether it is the Department's or that of another organization.
- ❑ establish group passwords (for example, LAN passwords) for facilities or systems access.

PROCEDURES TO FOLLOW WHEN LEAVING EMPLOYMENT AT DFAIT

Regardless of the circumstances under which you leave your employment, it is important to understand and maintain your security obligations. Upon your departure from the Department, you are 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 and protected information, as well as any government assets and information acquired during your period of service.
- Return your ID card to the Identification Section in Room BG-180
- Complete form TBS-SCT330-25: Administrative Cancellation of RS/Security Clearance Form.
- Return your office keys to the Divisional Administrative Assistant or the person responsible for keys in your Section.