Ombudsman

Ministère de la Défense nationale et Forces armées canadiennes

Manuel de sécurité

2017

Ombudsman
National Defence and Canadian Forces / Défense nationale et Forces canadiennes

Table des matières

1 Introduction

Le présent manuel de sécurité est conçu pour aider les employés du Bureau de l'Ombudsman à exercer leurs responsabilités individuelles en matière de sécurité dans le travail qu'ils accomplissent chaque jour pour appuyer l'exécution du mandat de Bureau. En vertu de la Politique du gouvernement sur la sécurité, un bureau fédéral doit protéger les biens (renseignements et technologies) qui lui sont confiés.

Le manuel donne des lignes de conduite touchant la classification des documents, le marquage de sécurité, le courrier, la manutention, l'entreposage, la transmission et le transport, ainsi que d'autres aspects d'intérêt professionnel liés à la sécurité des employés du Bureau de l'Ombudsman. L'adresse de sites Internet est également donnée pour prendre connaissance des politiques ou pour se renseigner davantage.

Pour plus d'information sur les exigences en matière de sécurité, n'hésitez pas à communiquer avec votre supérieur, le surveillant de la sécurité de l'unité ou le groupe des services juridiques.

L'Ombudsman,

Gary Walbourne

1.1 Modifications

Section	Changements apportés
Table des matières	Nouveau logo
3.1 Classification des Documents	3.1.1 Introduction : ajout d'hyperliens vers la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*.
	3.1.2 Information classifiée/désignée : Hyperliens mis à jour vers les politiques gouvernementales sur la sécurité et la sécurité de l'information (Ordonnances et directives de sécurité de la Défense nationale). Ajout d'un hyperlien vers l'annexe A.
3.2 Marquage	Référence vers l'ICP (hyperlien ajouté).
	Lien ajouté vers les politiques internes de GI.
3.3 Accès	3.3.1 Accès aux documents : Nouveau lien vers le Guide de l'équipement de sécurité.
	3.3.2 Zones d'accès : La zone de réception est maintenant un point d'accès au bureau uniquement.
	3.3.3 Cartes d'identité/laissez-passer : Retrait de la mention de la passe RCN NDI 80. Ajout d'un lien vers la directive de sécurité numéro 7 du MDN. Inclusion des laissez-passer temporaires.
	3.3.4 Visiteurs : On ne fait plus mention de la réception. Mention des commissionnaires en ce qui concerne la signature du registre. Ajout d'un lien vers la Politique sur la sécurité du gouvernement et la Politique de la Défense nationale en matière de sécurité. Ajout d'un lien vers l'annexe B et vers le formulaire sur le disque o:.
3.4 Filtrage de sécurité	3.4.1 Cote de fiabilité et Autorisation de sécurité : Mise à jour concernant les vérifications de la fiabilité. Retrait de la mention de ressources humaines. Mise à jour du lien vers la norme sur les vérifications de sécurité.

	3.4.3 Refus : Mise à jour du lien vers la norme sur les vérifications de sécurité.
	3.4.5 Transfert/réactivation de la cote : Ajout d'un hyperlien vers les formulaires de sécurité 330-23 et 330-60.
3.8 Destruction	Lien vers les IPO internes.
3.9 Téléphones	Retrait de l'interdiction des appareils Bluetooth avec les téléphones cellulaires.
3.10 Télécopieurs	Retrait de la mention de la page couverture des télécopies et du lien connexe, puisqu'elle n'est plus en usage. Retrait de la mention du télécopieur de niveau secret puisqu'il n'est plus en usage.
3.11 Ordinateurs portatifs et de bureau	Retrait de la mention du poste TEMPEST puisqu'il n'est plus en usage.
3.13 Ordinateurs de table	3.13.2 Mots de passe : Hyperlien vers l'annexe C. Ajout d'information sur les mots en passe en général.
	3.13.3 Exposés sur les comptes réseau : Lien vers la DOAD 6002-2.
	3.13.4 Courriels : Hyperlien vers l'annexe J
3.14 Clés USB/CD/DVD	Hyperlien vers l'annexe D Ajout de la mention de téléphones et tablettes personnels.
3.16 Infractions à la sécurité	Hyperlien vers l'annexe I
3.19 Sécurité physique	3.19.1 Boutons d'alarme : Mise à jour incluant l'éclairage intermittent.
	3.19.2 Programme des niveaux d'alerte de sécurité : Ajouté. Hyperliens vers les sections 3.20.2 Menaces et 3.20.8 Lettres ou appels menaçants ou malveillants du *Manuel de sécurité*. Ajout d'un hyperlien vers l'annexe F.
3.20 Mesures d'urgence	3.20.1 Mesures d'urgence : Lien vers l'annexe H et lien vers la politique sur les petits appareils électriques.
	3.20.6 Substances ou objets suspects : ajout d'un hyperlien vers l'annexe F.
	3.20.7 Alertes à la bombe : Ajout d'un hyperlien vers l'annexe E.
	3.20.8 Lettres ou appels menaçants ou malveillants : Ajout de l'annexe F.
Annexe B : Formulaire de	Ajout du nouveau logo.

réunion	Retrait des coordonnées de la réception.
Annexe C : Protection des documents par mot de passe	Mise à jour pour refléter notre version actuelle de Word et d'Excel.
	Nouvelles captures d'écran.
Annexe D : Balayage de clés USB, de CD, de DVD, etc.	Processus d'exécution mis à jour.
	Retrait de la mention de disquettes.
Annexe F (retirée) : Anthrax	Retrait complet du Manuel.
Annexe F (nouvelle) : Alerte à la bombe	Image améliorée.
Annexe H : Procédure d'appel nominal	Retrait de la mention de la réception.
Annexe I : Vérifications de sécurité	Ajout d'hyperliens vers les sections 3.15 et 3.5.1 du *Manuel de sécurité*.
Annexe J : Bloc de signature normalisé	Hyperlien vers l'annexe E : Blocs-signatures du courriel. Mise à jour de certaines exigences et du modèle de signature.
Glossaire	Ajout d'un glossaire.

2 Responsabilités ministérielles

En matière de sécurité, il incombe au Bureau de l'Ombudsman de :

- protéger les renseignements et les biens qui lui sont confiés;
- sauvegarder le caractère confidentiel, l'intégrité et la valeur des renseignements;
- respecter les exigences des directives ministérielles et de la Politique du gouvernement sur la sécurité;
- protéger les employés de menaces liées au travail;
- veiller à la prestation continue des services et à la planification de la poursuite des activités.

2.1 Gestionnaires

Il incombe aux gestionnaires de :

- veiller à ce que les particuliers obtiennent la cote de sécurité nécessaire avant d'assumer leurs fonctions;
- rester vigilants et prendre les mesures nécessaires à la suite de toute nouvelle information qui pourrait mettre en péril la fiabilité ou la loyauté d'un particulier ayant obtenu la cote de sécurité;
- déclarer sans tarder un incident portant atteinte à la sécurité et mettre en place les mesures nécessaires pour empêcher que l'incident se reproduise;
- veiller à mettre en œuvre dans leur section respective les mesures de sécurité décrites dans le présent document.

2.2 Employés

Il incombe aux employés et à toute personne travaillant dans le Bureau de :

- suivre les lignes de conduite établies dans le manuel de sécurité;
- protéger les biens sous leur garde conformément à la présente politique;
- déclarer à leur supérieur ou au surveillant de la sécurité de l'unité, le plus tôt possible, les menaces pesant sur leur sécurité ou d'autres incidents portant atteinte à la sécurité. Veuillez vous référer au programme des niveaux d'alerte de sécurité (section 3.19.2).

2.3 Surveillant de la sécurité de l'unité

Le surveillant de la sécurité de l'unité (SSU) est le coordonnateur désigné en matière de sécurité pour le Bureau. Il lui incombe :

- d'informer la direction au sujet des questions de sécurité;
- d'aider les particuliers ayant des préoccupations concernant la sécurité et des questions sur la présente politique;
- de veiller à ce que la présente politique soit tenue à jour et corresponde à l'état actuel de la Politique du gouvernement sur la sécurité;
- De fournir des mises à jour ainsi que des sessions de formation et de sensibilisation lors de rencontres de tout le personnel.

NOTA – En l'absence du SSU, son remplaçant agit à titre de personne-ressource.

3 Protection des renseignements

3.1 Classification des documents

3.1.1 – Introduction

Les renseignements de nature délicate font habituellement l'objet d'une exception en vertu de la *Loi sur l'accès à l'information* (*LAI*) ou de la *Loi sur la protection des renseignements personnels* (*LPRP*). Ils doivent être catégorisés comme classifiés ou désignés, et marqués du niveau de classification ou de désignation nécessaire.

La *LAI* donne aux citoyens canadiens un droit d'accès à l'information contenue dans les dossiers du gouvernement fédéral.

La *LPRP* confère aux citoyens un droit d'accès à l'information que le gouvernement possède à leur sujet et protège cette information contre toute utilisation ou divulgation non autorisée.

Le site Web suivant renseigne davantage sur la *LAI* et la *LPRP* : http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/index-fra.asp.

3.1.2 – Renseignements classifiés ou désignés

Les renseignements classifiés sont liés à l'intérêt national et touchent la défense et la sauvegarde de la stabilité sociale, politique et économique du pays. Voici les niveaux de classification :

- **Confidentiel** – une atteinte à l'intégrité des renseignements (notamment les tactiques de combat, les doctrines tactiques, les détails touchant le tableau des effectifs de guerre d'une unité) est vraisemblablement susceptible de causer un préjudice à l'intérêt national;

- **Secret** – une atteinte à l'intégrité des renseignements (notamment les documents confidentiels du Cabinet, les détails touchant le tableau des effectifs de guerre des FC, le déploiement des forces remplissant un rôle opérationnel, les détails sur l'équipement cryptographique) risquerait vraisemblablement de porter un sérieux préjudice à l'intérêt national;

- **Très secret** – une atteinte à l'intégrité des renseignements (notamment les éléments de décryptage, de guerre électronique et des plans de guerre) risquerait vraisemblablement de causer un préjudice exceptionnellement grave à l'intérêt national.

Les renseignements désignés ne sont pas liés à l'intérêt national, mais ils sont d'intérêt personnel et privé. Voici les niveaux de désignation :

- **Protégé A** – renseignements de nature peu délicate, notamment le nom et l'adresse de particuliers, etc., où le risque de péril causé par l'atteinte à l'intégrité serait minimal;

- **Protégé B** – renseignements de nature particulièrement délicate, notamment des renseignements médicaux, financiers, etc., où la divulgation pourrait causer un préjudice grave mais non lié à l'intérêt national;

- **Protégé C** – renseignements de nature extrêmement délicate, notamment de nature criminelle, risque pour la vie, etc., où la divulgation pourrait causer un préjudice très grave mais non lié à l'intérêt national.

Un tableau sommaire sur les détails qui précèdent figure à l'annexe A.

Veuillez noter que les renseignements soumis au secret professionnel des avocats doivent être désignés Protégé B et être traités en conséquence.

Pour plus d'information sur la définition des renseignements classifiés ou des renseignements désignés, n'hésitez pas à communiquer avec votre supérieur ou le SSU. Il y a aussi de nombreuses ressources à consulter sur le sujet, notamment :

Conseil du Trésor : Politique sur la sécurité – Guide du gestionnaire
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

Instructions de sécurité de la Défense nationale – chapitre 6 des Ordonnances et directives de sécurité de la Défense nationale

http://www.vcds.mil.ca/sites/intranet-fra.aspx?page=18369

3.2 Marquage

Il incombe aux rédacteurs ou aux expéditeurs de déterminer si le contenu des documents constitue des renseignements classifiés ou désignés. Les documents doivent être marqués de la cote de sécurité la plus élevée qui correspond au niveau de classification ou de désignation de leur contenu ou de leurs pièces jointes.

Le marquage doit figurer à l'angle supérieur droit de chacune des pages.

Le même document ne peut pas porter à la fois une marque de classification et une marque de désignation.

On ne doit pas confondre la marque de sécurité « confidentiel » avec la marque « personnel et confidentiel », conçue pour sauvegarder l'aspect personnel des renseignements ou l'aspect commun restreint. (Les formulaires de congé peuvent être considérés comme confidentiels mais sont marqués « Protégé B » aux fins de sécurité.) Le Bureau ne détient que très rarement des documents à renseignements désignés « Protégé C » ou classifiés « Très secret ». Ces documents devraient être marqués, entreposés et gérés à la suite d'une consultation avec le SSU.

Pour plus d'information sur la ligne de conduite à suivre en matière de marquage, veuillez communiquer avec votre gestionnaire ou le SSU, et consulter le site Web suivant :
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12333

On ne devrait pas avoir recours aux courriels pour communiquer des renseignements ou documents délicats. Cependant, les documents Protégé B peuvent être envoyés par le réseau s'ils sont cryptés à l'aide de l'infrastructure à clé publique (ICP). L'information ou les documents qui contiennent des renseignements plus délicats que Protégé B ne peuvent être envoyés par courriel, même s'ils sont cryptés à l'aide d'une carte ICP.

Dans certains cas, des biens autres que des documents pourraient devoir être marqués ou étiquetés en raison de leur nature délicate, notamment :

- la combinaison des armoires de sécurité pour les documents classifiés ou désignés ou les biens de valeur;
- les mots de passe pour accéder à des systèmes d'entreposage de données de nature délicate.

Le SSU est seul responsable de ces cas. Voir les politiques de GI pour des renseignements et directives supplémentaires.

3.3 Accès

3.3.1 Accès aux documents

Seuls peuvent avoir accès aux documents classifiés ou désignés les particuliers qui, dans l'exercice de leurs fonctions, ont un besoin de savoir légitime **et** la cote de sécurité de niveau voulu.

Les renseignements ne devraient pas être divulgués à quiconque n'a pas un besoin de savoir légitime.

Vous devriez veiller à ce que les documents qui vous ont été confiés soient entreposés dans une armoire verrouillée qui convient au niveau de sécurité. Pour plus d'information sur la ligne de conduite à suivre en matière d'entreposage dans une armoire verrouillée, veuillez communiquer avec le SSU ou consulter la page Web suivante :
http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm

3.3.2 Zones d'accès

Seuls les employés et les individus ayant reçu du gestionnaire compétent ou du SSU une autorisation particulière de circuler dans le Bureau peuvent accéder librement aux zones occupées. Les visiteurs doivent être accompagnés par un employé en tout temps.

Les employés et les particuliers ayant reçu l'autorisation de circuler dans le Bureau doivent interroger les individus qu'ils ne reconnaissent pas et qui cherchent à entrer ou qui sont entrés. Toute tentative d'entrée non autorisée doit être déclarée immédiatement au SSU.

ZONE	Bureau de l'Ombudsman
Réception	Pendant les heures ouvrables, des agents de sécurité postés aux entrées d'immeuble et des lecteurs de cartes d'accès contrôlent l'accès. En autre temps, le contrôle se fait grâce aux portes verrouillées, aux lecteurs de cartes d'accès et à la patrouille de surveillance. Les zones de réception sont publiques, conçues pour l'accueil des visiteurs et recevoir le courrier. L'accès aux bureaux des 12e et 13e étages est contrôlé par lecteur de carte depuis les couloirs d'ascenseur jusqu'aux espaces de bureau.
Opérations	L'accès aux zones de travail, situées après la réception et avant les zones de sécurité, est contrôlé aux zones de la réception et est réservé aux particuliers ayant une carte d'accès et, pendant les heures ouvrables, aux visiteurs autorisés accompagnés d'un employé. Ces zones constituent la majeure partie de l'espace occupé par le Bureau. Y

	sont traités et entreposés les documents de niveau Protégé A, Protégé B et Confidentiel.
Sécurité	Ces zones sont normalement encloisonnées, p. ex., la salle des dossiers et la salle du serveur de TI. Pendant les heures ouvrables, l'accès y est strictement contrôlé, et seuls les employés travaillant dans la zone et les visiteurs autorisés accompagnés y ont accès. En autre temps, l'accès se fait sous autorisation seulement.

3.3.3 Cartes d'identité ou laissez-passer

Quartier général de la Défense nationale (QGDN)

Les particuliers qui travaillent au Bureau de l'Ombudsman reçoivent du QGDN une carte d'identité et/ou un laissez-passer d'immeuble qu'ils doivent montrer sur demande à l'agent de sécurité de l'immeuble ou à d'autres individus aux installations visitées. Certains édifices sont équipés d'engins pour que les particuliers y glissent leur laissez-passer et entrent un NIP afin de pouvoir entrer.

- Les personnes employées pour une durée indéterminée reçoivent un laissez-passer d'immeuble de la RCN et une carte d'identité NDI 21.

- Les autres personnes reçoivent seulement un laissez-passer d'immeuble de la RCN ou un laissez-passer du Bureau de l'Ombudsman.

Les employés indéterminés peuvent utiliser leur carte NDI 21 pour être admis dans n'importe quel bâtiment du MDN dans la RCN, s'ils ont besoin de s'y rendre. Ils peuvent se faire demander de montrer leur carte NDI 21 lorsqu'ils circulent dans un édifice du MDN. Pour cette raison, cette carte devrait toujours être en votre possession.

Urbandale

Des lecteurs de cartes d'accès électroniques servent à contrôler l'accès pendant les heures ouvrables et/ou en dehors des heures ouvrables. Le SSU émet ces cartes et en interdit l'usage commun ou le prêt.

Les particuliers doivent prendre les mesures nécessaires pour empêcher la perte ou le vol de la carte qui leur est confiée, ou son usage par une autre personne. La perte ou le vol doit être immédiatement déclaré au SSU. Le particulier qui cesse de travailler au Bureau doit remettre sa carte au SSU.

Le SSU dispose de laissez-passer temporaires destinés aux militaires et aux entrepreneurs qui doivent avoir accès au Bureau pendant les heures ouvrables. Une

évaluation détermine si l'on doit accompagner ces particuliers ou si un laissez-passer leur est émis. En autre temps, on doit communiquer avec le SSU. Une surveillance et un contrôle rigoureux sont nécessaires quant à l'émission de laissez-passer à des personnes autres que des employés, et le laissez-passer doit être remis une fois satisfait le besoin en matière d'accès.

Le SSU dispose de laissez-passer temporaires, lesquels doivent être remis dans les 24 heures, pour le particulier qui aurait oublié le sien.

Les laissez-passer endommagés ou défectueux peuvent être remplacés auprès du SSU.

Voir la Directive de sécurité numéro 7 (http://vcds.mil.ca/sites/intranet-fra.aspx?page=14830) du MDN pour en savoir plus sur les laissez-passer octroyés par le MDN.

3.3.4 Visiteurs

Les visiteurs doivent se présenter au bureau des commissionnaires à l'entrée du bâtiment. Une fois leur rendez-vous confirmé, les visiteurs reçoivent une carte de visite et signent le registre des commissionnaires. Tous les visiteurs doivent être escortés, à partir de l'entrée principale, et ce, jusqu'à leur départ, par la personne qu'ils visitent. Une fois admis, les visiteurs sont à la charge de la personne qui a autorisé la visite.

L'enregistrement des visiteurs est une pratique courante dans l'ensemble du gouvernement. Au MDN, il faut s'enregistrer à l'entrée de tout bâtiment auquel on n'a pas accès. Le Bureau de l'Ombudsman doit assurer la confidentialité de toutes les plaintes qu'il reçoit. Ainsi, toute personne qui n'est pas employée par l'Ombudsman doit être enregistrée et escortée. Cela comprend notamment les employés du MDN et les militaires, ainsi que les personnes qui visitent des employés pour des motifs personnels (conjoints, enfants, etc.). De nombreuses politiques gouvernementales soutiennent cette pratique, notamment la Politique sur la sécurité du gouvernement et la Ordonnances et directives de sécurité de la Défense nationale. Les politiques de sécurité Urbandale, mises en place par le service de sécurité de Services publics et Approvisionnement Canada (SPAC), qui est responsable de la sécurité de l'édifice Urbandale, exigent aussi la tenue d'un registre pour tous les visiteurs qui ne travaillent pas à Urbandale.

Plusieurs raisons justifient cette pratique. En voici quelques-unes.

Le Bureau est responsable de la sécurité de tous les visiteurs qu'il reçoit à ses étages. En cas d'urgence, nous sommes en mesure d'assurer l'évacuation sécuritaire de nos visiteurs grâce à nos préposés aux urgences et pouvons confirmer qu'ils sont en sûreté à l'aide de l'appel nominal.

L'enregistrement des visiteurs nous permet aussi de protéger nos ressources. Si des ressources/équipements/documents ou des dossiers disparaissent pendant ou après les heures de bureau, le registre des visiteurs nous permet de savoir qui était présent dans le bureau et à quel moment, si une enquête devait avoir lieu ultérieurement.

La protection du personnel est très importante. Si une atteinte à la sécurité impliquant des visiteurs survient, le registre nous permet de connaître le nom des visiteurs et l'heure de leur arrivée/départ. Il permet aussi au personnel de distinguer les employés des visiteurs.

Les organisateurs de réunions ou de visites en groupe doivent prévenir les commissionnaires en remplissant le formulaire sur le lecteur commun O:\. Une copie du formulaire doit être remise au bureau des commissionnaires.

Le formulaire se trouve dans le dossier O:\Administration\Administration Forms\Security. Voir aussi l'annexe B.

Pour des raisons de sécurité, l'accès au Bureau en dehors des heures ouvrables par des personnes autres que les employés n'est pas encouragé. Les employés qui veulent demander un accès doivent obtenir une permission écrite explicite de leur gestionnaire. Le SSU doit aussi être informé de la visite pour la consigner au registre.

3.3.5 Entrée furtive

Tous les employés doivent veiller à ce qu'aucune personne non autorisée n'entre dans le bâtiment en dehors des heures ouvrables. Si vous entrez dans le bâtiment durant la fermeture des bureaux et qu'une personne inconnue tente d'entrer derrière vous, vous devez lui demander d'utiliser sa carte d'accès au bâtiment. Même si elle possède une carte d'identité d'un ministère, cette personne n'a peut-être pas l'autorisation d'entrer dans le bâtiment en dehors des heures ouvrables.

Tous les employés doivent s'assurer que quiconque sort de l'ascenseur au 13e étage est un employé de l'Ombudsman. L'accès non accompagné au 13e étage est interdit à quiconque n'est pas un employé de l'Ombudsman.

3.4 Filtrage de sécurité

3.4.1 Cote de fiabilité et autorisation de sécurité

L'exigence relative à la cote de fiabilité ou à l'autorisation de sécurité doit figurer dans les descriptions de travail, les documents de dotation et les documents contractuels. Quiconque reçoit une offre d'emploi, de contrat ou d'affectation doit

avoir obtenu au préalable une vérification approfondie de la fiabilité du MDN et obtenir l'autorisation de sécurité nécessaire au poste dans le cas échéant.

L'exécution d'une vérification approfondie de la fiabilité est une bonne pratique d'embauchage. Elle sert à établir la fiabilité d'un particulier avant l'embauche et comprend une vérification du casier judiciaire et une vérification de la solvabilité.

Le particulier doit donner son consentement par écrit pour que les renseignements servant à la vérification soient recueillis, à défaut de quoi sa candidature à l'emploi, au contrat ou à l'affectation est refusée.

Une vérification des données personnelles et professionnelles est nécessaire pour obtenir une cote de fiabilité. Le gestionnaire doit effectuer une vérification de la scolarité, des adresses et d'emplois antérieurs, et de l'identité, puis communiquer avec le SSU pour compléter les formulaires nécessaires et ainsi confirmer l'exécution de la vérification.

La Norme sur la sécurité du personnel dans la Politique du gouvernement sur la sécurité est utile à titre de ligne de conduite pour l'exécution des vérifications. http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115

3.4.2 Renouvellements

Le SSU amorce le processus de renouvellement de la cote de sécurité et demande aux particuliers une mise à jour des renseignements servant à la vérification. La cote de fiabilité et la cote de sécurité de niveaux I et II doivent être renouvelées tous les dix ans, et la cote de sécurité de niveau III tous les cinq ans.

3.4.3 Refus

Voir l'appendice D, article 18 de la Norme sur la sécurité du personnel dans la Politique du gouvernement sur la sécurité pour des renseignements sur le refus, la révocation ou la suspension des cotes de sécurité.
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115

3.4.4 Présentation du profil de sécurité

Tout employé du Bureau doit être informé en matière de cote de fiabilité et d'autorisation de sécurité. Le SSU donne au nouvel employé un exposé au début de l'embauche.

3.4.5 Transfert/réactivation de la cote

Un militaire qui entre en poste dans notre organisation sans avoir interrompu son service pendant 24 heures ou plus peut faire transférer/réactiver sa cote de sécurité en vigueur dans son emploi civil (son CIDP remplacera son numéro matricule) sans refaire tout le processus de vérification. Toutefois, ce processus exige tout de même de remplir les formulaires de sécurité 330-23 et 330-60 le cas échéant. Ces formulaires servent à mettre à jour le statut d'emploi, le lieu de résidence, l'état civil et tout autre renseignement qui a pu changer depuis la dernière vérification.

3.5 Clés et combinaisons

Les employés ont la responsabilité de protéger les renseignements et l'équipement qui leur sont confiés, y compris les clés de bureau, les cadenas et les combinaisons. Les clés ne doivent pas être dupliquées et il faut déclarer immédiatement au SSU la perte ou le vol de l'une d'entre elles. Les cadenas et leurs combinaisons sont aussi la responsabilité des personnes à qui ils sont remis. Les combinaisons ne devraient pas être divulguées, révélées ou placées dans des endroits où elles pourraient être vues et utilisées par des personnes non autorisées. Tout incident doit être déclaré rapidement au SSU.

Le SSU distribue les clés de bureau et les cadenas. L'utilisateur du cadenas configure la combinaison et en donne une copie au gestionnaire et au SSU. Le gestionnaire veille à ce que la combinaison soit changée soit au départ de l'employé, lorsque l'employé n'a plus besoin de l'accès ou si la combinaison secrète a pu être compromise. Les personnes qui reçoivent des classeurs avec serrure à combinaison intégrée doivent s'assurer que la combinaison est changée tous les six mois, que le changement est consigné sur une carte de suivi conservée à l'intérieur du classeur et qu'une copie est remise au SSU. Aux fins d'audit, le SSU peut demander à voir le registre des changements de combinaison en tout temps. Le SSU tient à jour un registre de clés et de combinaisons.

Les gestionnaires doivent aussi garder une liste des combinaisons utilisées par leurs subordonnés dans une enveloppe scellée sous le contrôle d'une seule personne, dans une armoire verrouillée conçue pour l'entreposage des renseignements auxquels les clés ou les combinaisons donnent accès. L'enveloppe est marquée du niveau de sécurité correspondant aux renseignements entreposés dont le niveau est le plus élevé.

Veuillez consulter la Norme sur le filtrage de sécurité du Conseil du Trésor à l'adresse suivante :
http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115

Les formulaires et les enveloppes nécessaires peuvent être obtenus du SSU.

3.6 Entreposage

3.6.1 Poste et zone de travail

Il incombe aux employés de veiller à la sécurité de leur zone de travail. Les postes et zones de travail doivent être le plus possible propres et sécuritaires pendant les heures ouvrables. Il faut les sécuriser le soir en quittant le bureau (y compris les corbeilles à recyclage et à ordures, de même que les boîtes de réception et de courrier).

3.6.2 « Sous verrou »

Selon le *Guide de l'équipement de sécurité* de la GRC, les renseignements désignés Protégé A et Protégé B, accessibles seulement aux particuliers ayant besoin d'en prendre connaissance, doivent être « sous verrou » dans la zone de travail pendant les heures ouvrables.

Par conséquent, si un employé doit s'absenter de courtes durées de son poste de travail pendant les heures ouvrables, il lui suffirait peut-être d'éloigner du regard les documents (soit tourner les pages de matériel de nature délicate, les mettre dans un dossier vierge, dans un tiroir, ou fermer la porte du bureau). *Il incombe à la personne qui utilise les documents d'en assurer la sécurité.*

Nota : On recommande de verrouiller l'écran de l'ordinateur au moment de s'absenter de son poste et de ne pas laisser le délai de la fonction de temporisation prendre fin. Cela évitera que des personnes non autorisées voient les documents à votre écran.

L'employé qui prévoit s'absenter longuement de son poste de travail pendant les heures ouvrables doit prendre les mesures de sécurité habituellement appliquées à la fin de la journée ou au moment de s'absenter plus longuement (comme pour partir en vacances, etc.).

Le lien suivant informe davantage sur la mise « sous verrou » :
http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm

Entreposage de documents non utilisés ou en dehors des heures de travail

Classification/Désignation	Exigences en matière d'entreposage
Protégé A	Armoire verrouillée
Protégé B	Armoire munie d'une serrure à combinaison ou d'un cadenas à clé approuvé
Protégé C	Selon les recommandations du SSU

Classification/Désignation	Exigences en matière d'entreposage
Confidentiel	Armoire munie d'une serrure à combinaison, ce qui exclut le classeur de votre bureau. Consultez le SSU pour vérifier les exigences d'entreposage. Nous avons un classeur approuvé pour le rangement de ce type de données.
Secret	Armoire munie d'une serrure à combinaison, ce qui exclut le classeur de votre bureau. Consultez le SSU pour vérifier les exigences d'entreposage. Nous avons un classeur approuvé pour le rangement de ce type de données.
Très secret	Selon les recommandations du SSU

3.6.3 Entreposage sur rayons ouverts

L'entreposage de renseignements désignés ou classifiés sur rayons ouverts ou l'entreposage en vrac de biens de valeur (p. ex., ordinateurs, équipement dispendieux ou essentiel) doit se faire dans des pièces à accès réservé. Ces pièces sont construites en fonction du niveau de confidentialité des renseignements qui s'y trouvent ou de l'importance des biens entreposés. L'accès à ces pièces est strictement contrôlé.

3.6.4 Affiche « Titulaire absent »

Les particuliers devraient utiliser l'affiche « Titulaire absent », fourni par le SSU, pour empêcher qu'on laisse des documents de nature délicate sur leur bureau lorsqu'ils sont absents. **On ne doit laisser aucun renseignement dans une poste de travail en l'absence de l'occupant.**

3.6.5 Biens personnels

Il incombe aux employés de protéger leurs biens personnels. Sacs à main, portefeuilles et argent devraient être gardés avec soi en tout temps ou mis dans une armoire ou une pièce verrouillée. Quand vous quittez votre poste de travail, veuillez vous assurer de ne pas laisser d'objets de valeur à la vue afin d'éviter les incidents. Le Bureau ne peut être tenu responsable de la perte de biens personnels tant que la procédure ci-dessus est appliquée.

3.7 Envoi de courrier

Les documents classifiés ou désignés qui sont envoyés par courrier doivent être emballés et transportés selon les directives figurant dans le tableau ci-dessous,

conformément à l'article 8.4 de la Norme de sécurité relative à l'organisation et l'administration du Conseil du Trésor.
http://tbs-sct.gc.ca/pol/doc-fra.aspx?id=12333&section=text

Marques	PROTÉGÉ A PROTÉGÉ B	CONFIDENTIEL ET SECRET	TRÈS SECRET ET PROTÉGÉ C
Emballage	1 enveloppe collée ou 1 boîte scellée simple, aucune marque de sécurité (une enveloppe réutilisable ou une chemise étiquetée suffit pour livraison à l'intérieur du Bureau)	À l'exception des envois à l'étranger (voir ci-dessous), 1 enveloppe collée ou 1 boîte scellée simple, aucune marque de sécurité (une enveloppe réutilisable ou une chemise étiquetée suffit pour livraison à l'intérieur du Bureau)	2 enveloppes collées; colis encombrant ou lourd enveloppé de deux épaisseurs scellées; mettre l'adresse sur les deux épaisseurs; marquer l'épaisseur intérieure de « Ne doit être ouvert que par »; inscrire l'envoi dans le registre des envois
Livraison interne	Par courrier interne.	Dans une enveloppe scellée, courrier interne.	Dans une enveloppe scellée, livraison par porteur.
Livraison dans la RCN	Dans un porte-documents approuvé, courrier de 1re classe ou services de messagerie avec mallette approuvée.	Services de messagerie détenant la cote Secret; dans une mallette de sécurité pour passer d'un immeuble à un autre. Courrier de 1re classe, dans deux enveloppes dont l'enveloppe intérieure est marquée de « Ne doit être ouvert que par »; inscrire l'envoi dans le registre des envois.	Services de messagerie détenant la cote Très secret; dans une mallette de sécurité verrouillée pour passer d'un immeuble à un autre**.**
Livraison à d'autres villes du Canada	Par courrier de 1re classe.	*Confidentiel* – courrier de 1re classe et enregistrement du transit et de la livraison, ou services de messagerie commerciale fiables. *Secret* – services de messagerie fiables et enregistrement du transit et de la livraison.	Par courrier recommandé.
Livraison à l'étranger	Par courrier de 1re classe ou, en cas d'urgence, par services de messagerie commerciale fiables.	Emballage et livraison semblable à celles des documents Très secret.	Services d'envoi diplomatique de sécurité; mettre l'adresse « Division de la distribution » (SBG) MAECI sur l'enveloppe extérieure; le destinataire et le marquage de sécurité ne

Marques	PROTÉGÉ A PROTÉGÉ B	CONFIDENTIEL ET SECRET	TRÈS SECRET ET PROTÉGÉ C
			doivent figurer que sur l'enveloppe intérieure; insérer entre les deux enveloppes le formulaire GC 44 « Note d'envoi et reçu »; sceller l'enveloppe intérieure (ou le papier d'emballage intérieur) avec du ruban de sécurité approuvé.

3.8 Destruction

Les documents désignés ou classifiés doivent être détruits au moyen d'un destructeur de documents conçu pour le niveau de sécurité attribué aux documents. Se renseigner auprès du SSU.

Le Bureau possède des déchiqueteuses approuvées (conformément au *Guide de l'équipement de sécurité* et à la Politique du gouvernement sur la sécurité) pour la destruction de petites quantités de documents classifiés « Secret » ou d'un niveau de sécurité moins élevé. Il faut communiquer avec le SSU pour la destruction de grandes quantités de documents de nature délicate, qui doit être faite conformément aux lignes directrices du gouvernement du Canada et aux IPO internes sur la GI.

Les sites Web suivants renseignent davantage sur le sujet :

- *Guide de l'équipement de sécurité* de la GRC, section 2
  http://www.rcmp-grc.gc.ca/physec-secmat/reslim/pubs/seg/html/page_0068_f.htm

- Politique sur la gestion de l'information
  http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/mgih-grdg_f.asp

- IPO interne sur la gestion de l'information touchant la destruction
  O:\RKI\SOPs\Managing Disposition

Les CD et DVD à renseignements de nature délicate doivent être détruits d'une façon approuvée. Il faut communiquer avec le SSU pour la destruction de disques durs et d'autres dispositifs électroniques à renseignements de nature délicate, y compris les cartes à mémoire de télécopieur.

Le SSU veille à ce que ces articles soient détruits dans une installation approuvée.

La politique suivante renseigne davantage sur le sujet :

- *Guide de l'équipement de sécurité* de la GRC, section 3 http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0069_f.htm

Pour plus d'information sur la destruction de documents de nature délicate, n'hésitez pas à communiquer avec le SSU ou le groupe des services juridiques.

3.9 Téléphones

Le risque d'écoute des communications téléphoniques par des particuliers non autorisés est présent. Les mesures suivantes aideront à réduire ce risque et le risque de divulgation non autorisée :

1. Les téléphones cellulaires ou sans fil, y compris les cellulaires intégrés aux dispositifs *BlackBerry*, ne doivent pas servir pour transmettre des renseignements de nature délicate. Ces téléphones exploitent des ondes radio facilement accessibles.

2. Dans les cas où un téléphone cryptophonique n'est pas nécessaire et où les appels sont faits en provenance ou en partance d'endroits en dehors de la région du système de central téléphonique, il faut prendre des mesures pour réduire le risque d'écoute dans le réseau local (RL). Évitez de discuter de matière de nature délicate ou ne vous y attardez pas et n'entrez pas dans les détails.

NOTA – Un téléphone de RL exploite une ligne téléphonique ordinaire par l'entremise d'une prise de téléphone. Il n'est pas de la catégorie des « sans-fil », p. ex., téléphone cellulaire, *BlackBerry*, téléphone satellite, etc.

3.10 Télécopieurs

Les communications par télécopieur empruntent la même voie que les communications par téléphone et sont sujettes au même risque d'interception, décrit dans la section précédente. De plus, une divulgation non autorisée pourrait avoir lieu si l'on signale le mauvais numéro. La quantité d'information qu'il est possible de communiquer par télécopieur est normalement plus importante et le contenu, plus précis que ce qui est discuté au téléphone. Par ailleurs, il est plus facile de photocopier l'information. Par conséquent, les exigences suivantes sont en vigueur :

- ne pas utiliser un télécopieur pour l'envoi de tout renseignement classifié ou Protégé B;

- faire preuve de prudence en envoyant par télécopieur des renseignements de nature moins délicate, notamment désigné Protégé A ou non Sans classification, en veillant à ce que ce soit le destinataire prévu qui reçoive les renseignements.

3.11 Ordinateurs portatifs et de bureau

Seuls les ordinateurs équipés de logiciels de protection approuvés doivent servir au traitement des renseignements de nature délicate. En d'autres mots, vous n'êtes pas autorisés à utiliser votre ordinateur personnel pour traiter ces renseignements.

NE PAS se servir d'un ordinateur pour faire le traitement des renseignements Très secret, Secret et Protégé C. Consultez le SSU pour le traitement électronique de renseignements classifiés Secret et Confidentiel

Quand un utilisateur travaille sur un ordinateur portable (OP), pour traiter de l'information Protégé B, il doit utiliser uniquement un ordinateur Protégé A ou Protégé B (et non un ordinateur personnel). Les lignes directrices suivantes doivent être respectées :

les renseignements Protégé B ne peuvent être stockés sur un ordinateur Protégé A. Il faut utiliser une clé USB fournie par le Bureau pour y stocker l'information quand on a fini de l'utiliser.

- il faut utiliser sa carte ICP de concert avec un OP Protégé B afin d'accéder au système;

- ne sauvegarder aucune information sur le disque dur de l'OP;

- aucune transmission électronique n'est permise à partir de l'OP Protégé B; s'il faut effectuer une transmission, les renseignements doivent être sauvegardés sur une clé USB, puis transmis par un OP Protégé A dans un courriel chiffré au moyen du système ICP/Entrust;

- tout enregistrement du mot de passe doit être tenu séparé de la carte IPC; le mot de passe devrait être mémorisé; ne pas laisser l'OP sans surveillance après y avoir fait entrer la carte et avoir saisi le mot de passe;

- retirer la carte de l'OP après usage et l'entreposer dans une mallette ou un classeur approuvé; mettre l'OP dans un autre endroit verrouillé qui garantit suffisamment de protection contre tout accès non autorisé;

- sécuriser toute clé USB à renseignements de nature délicate et tout document imprimé à partir de l'OP dans une mallette ou un classeur approuvé;

- garder l'OP avec soi pendant le transport; si possible, transporter la carte ICP dans une mallette et garder la mallette avec soi ou dans un endroit sécurisé; en avion, l'OP devrait voyager dans la soute à bagages et la mallette avec soi;

- transporter les clés USB séparément de l'OP;

- au Bureau, entreposer l'OP dans une armoire de sécurité verrouillée;

- en dehors du Bureau, garder l'OP avec soi ou l'entreposer dans un endroit sûr (p. ex., à l'abri des regards, comme dans le coffre de la voiture, dans un lieu sûr à domicile ou dissimulé dans la chambre d'hôtel);

- déclarer immédiatement au SSU tout incident, soupçonné ou réel, mettant en péril la carte ICP ou l'OP (p. ex., un accès non autorisé, la perte, le vol, le vandalisme); à la remise d'un OP au SSU, ce dernier veille à effacer toutes les données avant de le confier à un autre utilisateur.

3.12 Cartes d'infrastructure à clés publiques (ICP)/Entrust

Le Programme d'ICP du MDN est un système conçu pour le traitement et la transmission de renseignements Protégé B au moyen de matériel Protégé A. Tous les employés indéterminés du Bureau sont tenus d'avoir une carte ICP.

L'accord d'abonnement signé par l'utilisateur au moment de l'émission de la carte ICP stipule les conditions suivantes (citées de l'accord) que précise le règlement sur la sécurité :

a) l'utilisateur de la carte ICP doit détenir la cote de fiabilité approfondie;
b) le nom d'utilisateur et le mot de passe ne doivent pas être révélés à d'autres employés, et les outils d'authentification ou les autres dispositifs de sécurité TI sont pour son usage personnel seulement et doivent être en lieu sûr en tout temps;
c) la signature numérique est tout aussi contraignante juridiquement que la signature manuscrite;
d) l'utilisateur doit accéder seulement aux données nécessaires à l'exercice de ses fonctions et dont l'utilisation est autorisée, et/ou ne doit copier que ces données;
e) aucune personne non autorisée ne doit accéder aux ressources susmentionnées;
f) n'user des privilèges d'accès aux ressources que pour son usage autorisé;
g) toute information de domaine désigné et tout matériel de TI désigné auxquels l'accès est donné doivent être sécurisés conformément à la Politique

sur la sécurité du gouvernement et à la Politique ou aux Instructions de sécurité de la Défense nationale;

h) l'utilisateur est responsable des soins raisonnables à donner aux ressources sous sa garde;

i) l'utilisateur doit respecter toutes les conditions liées aux licences d'exploitation des logiciels relativement aux ressources ICP qui lui ont été confiées et auxquelles il a accès;

j) l'utilisateur contreviendrait au règlement si, sans autorisation légitime, il :
   - communiquait l'information à laquelle il a l'autorisation d'accéder,
   - utilisait cette information ou les ressources ICP à des fins autres que des fins autorisées,
   - détruisait ou modifiait les données,
   - rendrait les données absurdes, inutilisables ou inefficaces,
   - faisait obstacle à l'utilisation légitime des données, en interrompait le cours ou créait de l'interférence;

k) le programme d'ICP ne doit pas être tenu responsable d'éventuels dommages ou pertes des données personnelles de l'utilisateur, ou de la perturbation des activités personnelles de l'utilisateur à la suite de l'utilisation des ressources susmentionnées ou à la suite de la perte du privilège d'utilisation des ressources susmentionnées;

l) l'utilisateur assume toute la responsabilité de ses actions et sait que toute violation de l'esprit des règles d'accès relatives au programme d'ICP peut mener à la perte du privilège d'utilisation et à d'autres mesures;

m) l'utilisateur connaît son rôle et les responsabilités connexes et a reçu un exposé sur le sujet conformément aux procédures du programme d'ICP.

Le SSU est en mesure de renseigner l'utilisateur davantage sur l'utilisation des cartes ICP.

3.13 Ordinateurs de table

3.13.1 Fonction de temporisation

Les systèmes Protégé A et Protégé B doivent être dotés d'une fonction de temporisation. Selon la politique du MDN, les paramètres de cette fonctionnalité ont été réglés d'avance en ce qui concerne le système Protégé A et ne peuvent pas être modifiés. Les paramètres du système Protégé B ont été réglés sur ceux du système Protégé A. Toutefois, il est recommandé de ne pas attendre le verrouillage automatique du système. Si vous quittez votre poste, vous devriez verrouiller votre écran afin d'empêcher quiconque de voir ce qu'il y a à l'écran ou d'utiliser votre poste.

3.13.2 Mots de passe

Il est de la responsabilité de tous de s'assurer que les mots de passe soient bien conservés et utilisés. Ne partagez pas vos mots de passe.

L'utilisation de mots de passe dans le traitement des documents *Word*, *Excel* ou autres est une façon de contrôler du partage des documents de nature délicate. Les mots de passe ne doivent pas figurer sur les documents ou circuler avec eux. Ils sont enregistrés par le gestionnaire aux fins de référence. Ceci est très important, surtout lorsque vient le temps pour un employé de quitter le Bureau.

L'annexe C décrit la façon de protéger un document au moyen d'un mot de passe.

3.13.3 Exposés sur les comptes réseau

Tous les utilisateurs doivent participer à un exposé sur les comptes réseau au moment d'accuser réception de leur compte. Les exposés sont donnés par le SSU. Les sites Web suivants renseignent davantage sur le sujet :

- Politique du Conseil du Trésor sur l'utilisation des réseaux électroniques : http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=27122

- DOAD 6002-2, Utilisation légitime d'Internet, de l'intranet de la défense, d'ordinateurs et d'autres systèmes de technologie de l'information : http://www.forces.gc.ca/fr/a-propos-politiques-normes-directives-ordonnances-administratives-defense-6000/6002-2.page

3.13.4 Courriels

Il est important de s'assurer d'envoyer les courriels aux destinataires voulus. Une façon de s'en assurer est d'ajouter les contacts fréquents à votre carnet d'adresses. Une autre méthode est de numériser votre liste et de vous assurer d'avoir les bons destinataires.

Le Bureau utilise un bloc de signature normalisé. Voir l'annexe J pour plus de renseignements.

En plus du bloc de signature normalisé, le Bureau a adopté un avertissement qui devrait être utilisé de pair avec la signature pour les nouveaux courriels, les réponses et les transferts de courriel.

L'avertissement devrait également être utilisé avec votre signature lorsque vous utilisez votre *BlackBerry*.

3.14 Clés USB, CD et DVD

Selon la politique du MDN, les clés USB personnelles, de même que les CD et DVD personnels (c.-à-d. ceux qui ne sont pas émis par le Bureau) ne doivent pas être utilisés avec les ordinateurs du MDN.

Veuillez noter que les clés USB, CD et DVD qui contiennent des renseignements Protégé A ou B ne doivent pas être branchées à des ordinateurs domestiques, y compris les ordinateurs autonomes Rogers du Bureau. Cette mesure est due à l'absence de mesures de sécurité protégeant l'information sur les ordinateurs domestiques. Ces ordinateurs sont exposés aux virus qui pourraient détruire ou compromettre les renseignements de nature délicate.

Les clés USB ne doivent pas être laissées branchées aux ordinateurs. Il faut les verrouiller quand elles ne sont pas utilisées.

Si une clé USB du Bureau contient uniquement du contenu sans classification et que vous la branchez sur un ordinateur domestique, vous devez balayer la clé en vue de la détection d'éventuels virus avant de la brancher à nouveau sur un ordinateur du Bureau. L'annexe D renseigne sur la façon de balayer les clés USB.

Le même principe s'applique à tout autre fichier électronique sauvegardé sur CD ou DVD. Ces supports doivent être balayés avant leur utilisation dans le système du MDN pour qu'aucun virus ne puisse se propager. Ils doivent également être protégés par mot de passe.

Il est interdit de brancher un téléphone ou une tablette personnel-le dans un ordinateur du MDN.

3.15 Renseignements de nature délicate en dehors du Bureau

Les employés dont le travail oblige à se déplacer en dehors du Bureau avec des renseignements de nature délicate doivent prendre les mesures nécessaires pour empêcher la divulgation de l'information en mettant cette dernière à l'abri du regard ou de l'écoute des personnes non autorisées. Ils doivent éviter les conversations portant sur les renseignements de nature délicate en présence de personnes non autorisées et s'entretenir de questions délicates seulement avec l'approbation de leurs gestionnaires.

Les mesures de protection suivantes s'appliquent aux renseignements de nature délicate désignés Protégé A et Protégé B :

En dehors du Bureau

Le particulier qui transporte des renseignements de nature délicate pour participer à des réunions en dehors du Bureau devrait :

- mettre les renseignements dans une mallette verrouillée et garder la mallette avec soi pendant le déplacement;

- pendant les pauses prolongées (p. ex., au dîner), entreposer la mallette ou les renseignements dans un endroit conçu pour l'entreposage de renseignements du niveau de sécurité pertinent ou apporter la mallette avec soi et la garder sous surveillance;

- pendant les séjours de plus d'une journée, entreposer la mallette dans un endroit sécurisé sur les lieux de la réunion ou, s'il est à l'étranger, la laisser à l'établissement de la mission diplomatique du Canada; en l'absence de lieu d'entreposage sécurisé, mettre les renseignements dans la mallette, verrouiller cette dernière et la mettre à l'abri du regard dans sa chambre d'hôtel ou dans son lieu d'accueil;

- ne pas traiter, entreposer ni transmettre les renseignements, ni en discuter, au moyen de systèmes (p. ex., ordinateurs, téléphones, télécopieurs) qui n'ont pas été approuvés pour le niveau de sécurité des renseignements.

À domicile

Les employés qui prévoient utiliser à domicile un ordinateur fourni par le Bureau devraient :

- en informer leur superviseur;

- transporter les renseignements dans une mallette verrouillée approuvée et les protéger contre toute divulgation non autorisée; les particuliers qui apportent souvent ce genre de renseignements à domicile doivent disposer d'une armoire de sécurité pour entreposer les renseignements.

  Nota : Ne pas révéler à quiconque la combinaison de la mallette.

3.16 Infractions à la sécurité

Une infraction à la sécurité est une activité qui permet de contourner les exigences de la politique de sécurité du Bureau et des règlements connexes, et qui pourrait porter atteinte à la sécurité.

Voici des exemples d'infractions : négliger d'entreposer des renseignements de nature délicate et de verrouiller les classeurs en dehors des heures ouvrables, négliger de protéger les cartes d'accès et les mots de passe, de transmettre et d'éliminer les renseignements conformément aux procédures de sécurité établies.

À la suite de contrôles de sécurité, un avis d'infraction est émis si les coffres de sécurité sont laissés déverrouillés, si le matériel de nature délicate n'est pas entreposé convenablement ou si, à la fin de la journée, les ordinateurs n'ont pas fait l'objet de la procédure de fin de traitement. Le SSU enlève le matériel non entreposé et le garde jusqu'à ce que l'employé qui en a la charge vienne le lui réclamer. Une copie de l'avis d'infraction est donnée au gestionnaire compétent et une autre est versée au dossier de sécurité de l'employé. Si un particulier reçoit plusieurs avis d'infraction, le SSU discute de mesures correctrices avec le gestionnaire.

Voir l'annexe I pour plus de renseignements sur les vérifications de sécurité.

3.17 Poursuite des activités

Un plan de poursuite des activités (PPA) est une stratégie de gestion du risque visant à limiter l'impact potentiel que des interruptions de service peuvent avoir sur les activités de l'organisation. Cette stratégie d'atténuation des risques est fondée sur l'idée que des interruptions de service surviendront. En conséquence, des plans doivent être établis, mis à l'essai, tenus à jour et mis à jour annuellement afin que le Bureau de l'Ombudsman puisse continuer de servir ses commettants.

Une urgence constitue une situation anormale qui exige des mesures en temps opportun pour limiter l'atteinte à l'intégrité des biens et les lésions que pourrait subir le personnel. Un accident chimique, biologique ou nucléaire, une cyberattaque, une panne de courant ou un désastre naturel (p. ex., séismes, inondations) peuvent tous être à l'origine d'une urgence.

La direction doit veiller à ce que des plans relatifs aux urgences et à la poursuite des activités, y compris un plan de secours en matière de TI ainsi que des procédures, soient mis au point, testés et mis à jour afin d'être en mesure de réagir aux urgences, de se rétablir et de continuer à assumer les fonctions critiques et à faire la prestation des services essentiels jusqu'à la reprise des activités normales. Il faut recenser les biens qui appuient les fonctions et les services essentiels, et déterminer les mesures à prendre qui en assurent la disponibilité dans l'éventualité d'une urgence. Des capacités de remplacement et le stockage hors place sont des éléments qui permettent la poursuite des activités.

Le plan de continuité des activités du Bureau de l'Ombudsman peut être consulté à l'emplacement suivant : O:\Administration\Security\Business Continuity Plan.

Veuillez noter que tous les membres du personnel doivent lire et comprendre le PPA. Il en va de leur propre intérêt et sécurité. Pour toute question sur le PPA et son contenu, veuillez contacter le coordonnateur du PPA, à savoir le directeur des services corporatifs, ou le SSU.

3.18 Enlèvement de biens

Les employés qui désirent déplacer un ordinateur ou un autre bien d'équipement de valeur en dehors des installations du Bureau doivent obtenir de leur gestionnaire une autorisation écrite ainsi qu'un formulaire du SSU. Ils pourraient devoir montrer l'autorisation au personnel de la sécurité de l'immeuble, et devraient garder l'autorisation sur leur personne chaque fois qu'ils entrent dans une nouvelle installation, car on pourrait leur demander de la produire à l'entrée de tout immeuble du gouvernement et d'attester que l'équipement appartient au MDN.

3.19 Sécurité physique

3.19.1 Boutons d'alarme

Il y a deux boutons d'alarme à la réception et dans la salle d'entrevue. Quand on les active, une lumière stroboscopique sera activée dans l'ensemble des 12e et 13e étages et les commissionnaires du lobby seront alertés. Ces derniers doivent :

1) appeler le 911;
2) aviser le superviseur de la sécurité de l'unité ou son remplaçant;
3) aviser les gestionnaires du bâtiment.

Vous ne devez utiliser les boutons d'alarme qu'en cas d'urgence.

Si vous activez un bouton accidentellement, veuillez appeler les commissionnaires sur-le-champ au 949-7243 pour leur indiquer qu'il s'agit d'une fausse alarme, puis appeler le superviseur de la sécurité de l'unité (ou son remplaçant) pour signaler l'incident.

En cas d'urgence réelle, une fois que le bouton est activé, veuillez tenter de vous retirer de la situation dangereuse. En quittant la salle, prenez une des enveloppes qui se trouvent près des sorties et qui contiennent les coordonnées de personnes à contacter en cas d'urgence. Si l'incident survient dans la zone de la réception, la personne doit entrer dans la zone des opérations en passant par la deuxième porte de la réception. Une enveloppe est située près de la sortie, qui contient les noms et numéros des personnes-ressources. Trouvez un téléphone et appelez le SSU. Le même processus s'applique si une situation survient dans la salle d'entrevue. La personne devrait sortir par la porte qui mène aux opérations et prendre l'enveloppe contenant les coordonnées d'urgence.

Si vous n'êtes pas en mesure de quitter le secteur en toute sécurité et sans laisser la personne menaçante pénétrer dans la zone des opérations, restez calme et souvenez-vous qu'en appuyant le bouton d'alarme, vous obtiendrez de l'aide.

Il faut noter que si vous entendez la sirène d'alarme dans un secteur, vous devez éviter d'y pénétrer. Soyez assuré que les autorités ont été alertées et que vous n'avez pas à intervenir.

VEUILLEZ NOTER QU'UN TEST DU SYSTÈME A LIEU CHAQUE ANNÉE. ON VOUS INFORMERA À L'AVANCE DE LA TENUE DU TEST.

3.19.2 Programme des niveaux d'alerte de sécurité

À la suite d'incidents passés, on a décidé que le Bureau devait se doter d'un programme des niveaux d'alerte de sécurité. Ce programme permettra au superviseur de la sécurité de l'unité de donner rapidement des renseignements au personnel quant aux menaces possibles et de gérer ces menaces du point de vue de la sécurité.

Conformément à la Politique du gouvernement sur la sécurité, la direction est chargée d'assurer un lieu de travail sûr à tous ses employés. Ce programme est approprié pour réagir aux types de menaces reçues tout en permettant la poursuite des activités quotidiennes du bureau. Il vise établir l'équilibre entre les exigences de sécurité et la nécessité d'efficacité et d'un certain degré d'ouverture envers les clients, les gens avec qui le Bureau interagit dans le cadre de ses activités et le public en général. Chaque niveau est associé à des mesures de sécurité plus rigoureuses qui peuvent être requises à des moments différents, pour répondre à des niveaux de menace accrus, que les menaces soient dirigées directement vers le Bureau ou non.

Le Bureau du Conseil privé peut apporter des changements au niveau de sécurité pour l'ensemble du gouvernement. Le superviseur de la sécurité d'unité pour le Bureau de l'Ombudsman, en consultation avec la haute direction, peut apporter des changements pour le Bureau. On s'attend à ce que les employés prennent connaissance de ces mesures. Ils doivent se plier aux mesures prises et contribuer à leur exécution.

La première partie de ce document est la procédure de signalement des incidents de sécurité réels ou potentiels, lesquels peuvent mener à l'élévation du niveau de sécurité du Bureau.

Signalement des incidents de sécurité

Les incidents de sécurité doivent être signalés de la façon suivante.

1) Ils doivent être signalés sur-le-champ au SSU (ou son remplaçant), par téléphone ou en personne.

2) Décrivez la situation à votre superviseur et dites-lui si vous avez avisé la sécurité.

3) Vous devriez demeurer disponible pour donner des renseignements au comité de sécurité ou aux services d'urgence, au besoin.

4) Restez calme et écrivez/documentez autant de détails possibles, notamment :
    - Nom/numéro de téléphone/adresse de la personne;
    - Date et l'heure de l'appel;
    - Endroit où se trouve la personne qui profère les menaces;
    - Tout ce que la personne dit – notamment les personnes vers qui sont dirigées les menaces.

**Les sections 3.20.2 à 3.20.8 du Manuel de sécurité donnent des détails sur la gestion des situations menaçantes*

***REMARQUE : En cas d'alerte à la bombe, la procédure à suivre est décrite à l'annexe F du présent document*

Mesures prises par le superviseur de la sécurité de l'unité :

- Aviser/rassembler les personnes concernées pour une réunion d'urgence – ces personnes sont les membres du comité de la haute direction et la personne qui a signalé l'incident;
- Décréter un niveau d'alerte de sécurité accru, au besoin;
- Informer le personnel du niveau de sécurité accru et transmettre l'information et les photos, le cas échéant, concernant l'incident en cours.

Mesures prises par le comité :

- Déterminer le niveau de menace et le risque pour les employés;
- Déterminer le niveau d'alerte de sécurité à mettre en place.

Alertes de niveau de sécurité

L'état par défaut et Vert. Le personnel sera avisé par téléphone ou en personne (ou par courriel si la menace n'est pas imminente) si des mesures plus rigoureuses sont décrétées et si ces mesures ont une durée déterminée.

Vert – Activités habituelles

- Certaines normes de sécurité courantes déjà en place :
    - Les commissionnaires vérifient les laissez-passer à l'entrée du lobby;
    - Des caméras de sécurité se trouvent dans le lobby du bâtiment ainsi qu'au 12e (réception et salle d'entrevue) et au 13e (près de la salle de conférence) étages;
    - Des boutons de panique se trouvent à la réception et dans la salle d'entrevue. Les employés doivent connaître leur emplacement et les utiliser si leur sécurité physique est menacée. Les employés devraient reconnaître le son produit quand un bouton d'alarme est activé et savoir quoi faire dans un tel cas;
    - Il y a un interphone à la réception;
    - La salle d'entrevue est contrôlée par un système à deux portes et un lecteur de carte;
    - Des lecteurs de carte activent toutes les portes sur les deux étages et, au 13e étage, celles des cages d'escalier et des ascenseurs.
- Des procédures de sécurité standards sont en vigueur aux deux étages.
- Tous les membres du personnel devraient avoir leurs cartes d'accès en leur possession en tout temps quand ils sont aux 12e et 13e étages. Ils devraient les porter visiblement quand ils sont dans le lobby ou à un autre étage que nous n'occupons pas.
    - Conformément à la Norme opérationnelle de sécurité – Niveaux de préparation des installations du gouvernement fédéral. http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12331
      Le gouvernement est actuellement au niveau de préparation 2, ce qui est sujet à changement.
- Les visiteurs doivent se présenter aux commissionnaires, à l'entrée principale, lesquels aviseront l'employé indiqué dans le formulaire de réunion. Voir l'annexe B.
    - Les visiteurs devraient être annoncés aux commissionnaires avant la tenue de la rencontre à l'aide du formulaire de réunion : O:\Administration\Administration Forms\Security
- Vous ne devez **jamais** laisser qui que ce soit franchir en même temps que vous un accès protégé par carte, que ce soit à l'entrée du bâtiment ou aux entrées/sorties des 12e et 13e étages.
- Les visiteurs entrent dans le lobby, signent le registre et obtiennent une carte de visiteur, puis sont escortés jusqu'aux bureaux par l'employé qu'ils sont venus rencontrer.
- Toutes les portes de la zone des opérations sont protégées par lecteur de carte.

12e étage – non sécurisé

- Ne laissez **personne** entrer en même temps que vous.

- Cette mesure vise à assurer la sécurité de tous.
- L'interphone de la réception, qui permet de communiquer avec les visiteurs, est une mesure de sécurité optionnelle.
- La salle d'entrevue doit être utilisée pour les plaintes en personne – les visiteurs ne doivent pas accéder au secteur des opérations. Ils doivent signer le registre, mais n'ont pas à porter une carte de visiteur. Le personnel doit conduire les plaignants à la salle d'entrevue en passant par la réception.

13e étage – sécurisé

- Accès protégé par lecteur de carte aux ascenseurs et dans les cages d'escalier.
- Les visiteurs du 13e étage doivent se rendre directement aux ascenseurs. On ne doit pas les laisser seuls à cet endroit.

Jaune – Avertissement

On doit évaluer chaque incident séparément afin de prendre les mesures de sécurité appropriées.

Toutes les précautions du niveau Vert s'appliquent, en plus des mesures suivantes :

- Le personnel doit se montrer vigilant envers toute personne et signaler la présence d'une personne indésirable au superviseur de la sécurité de l'unité et aux Services juridiques.
- Tous les employés recevront des photographies ou toute autre information pertinente concernant la situation en cours.

12e étage – non sécurisé/13e étage – sécurisé

- Bouclage de la réception
  - Les commissionnaires doivent escorter tous les visiteurs jusqu'au 12e/13e étage, y compris ceux qui ont une carte d'identité du MDN.
  - Les visiteurs ne doivent jamais être laissés sans surveillance.
  - Le courrier et les colis sont récupérés au lobby du 12e étage par le commis ou une autre personne désignée.
  - Des instructions seront données pour réagir aux appels menaçants ou aux personnes menaçantes qui tentent de pénétrer dans le bureau.
- Le SSU pourrait demander aux employés d'éviter d'utiliser la réception ou d'autres entrées afin d'éviter que des personnes s'infiltrent en même temps qu'eux dans la réception.

Rouge – Protocole de sécurité exhaustif

On doit évaluer chaque incident séparément afin de prendre les mesures de sécurité appropriées.

- Mesures de sécurité possibles :
  - Évacuation ou fermeture du bâtiment (bouclage complet);
  - Aucun visiteur admis dans le bâtiment ou aux 12e et 13e étages;
  - Présence possible de gardiens de sécurité aux 12e et 13e étages;
  - Activation possible du plan de poursuite des activités, selon la nature de l'incident;
  - Intervention des autorités, c.-à-d. police militaire (PM), police d'Ottawa, GRC.

Veuillez noter qu'en cas de niveau Rouge, diverses mesures de sécurité sont possibles. Ainsi, si le niveau Rouge est déclaré pour gérer un incident lié à la sécurité, des instructions précises sur les mesures prises seront transmises au personnel.

3.20 Mesures d'urgence

3.20.1 Mesures d'urgence

Consulter la description des mesures d'urgence Urbandale dans le dossier O:\Health and Safety\Emergency Procedures.

Il est à noter qu'en plus des mesures en cas d'incendie, le Bureau a mis en place une procédure d'appel nominal qui supplante les procédures de lutte contre les incendies du bâtiment. Ces procédures se trouvent à l'annexe H.

Dans les postes de travail ou les bureaux personnels, les chaufferettes, les cafetières et les plaques chauffantes de tout genre sont interdites.

Le SSU peut, au cas par cas, autoriser les ventilateurs à usage personnel.

Pour en savoir davantage sur ce qui est approuvé pour utilisation au Bureau, consulter la politique du Bureau concernant les petits appareils électriques, à l'adresse suivante :
O:\Health and Safety\Internal Programs & Policies\Small Appliance Policy\Politique sur les petits appareils électriques

Voir le superviseur de la sécurité de l'unité pour obtenir une autorisation.

3.20.2 Menaces

Il y a une variété considérable de motifs qui pousseraient un particulier à introduire dans un complexe immobilier du gouvernement un agent chimique, biologique, rayonnant ou explosif : acte terroriste, désir de causer un préjudice à un haut

fonctionnaire, de s'affirmer en influant négativement sur le fonctionnement du gouvernement, de causer du mal aux employés ou de contourner les mesures de contrôle.

Les menaces sont un fait concret de la vie moderne. Elles sont d'ordre mondial ou local, et peuvent viser un immeuble précis, un ministère ou des particuliers précis. Perçues ou réelles, les menaces représentent une préoccupation grave sur le plan de la sécurité et ont le potentiel de bouleverser le cours normal des activités.

Notre bureau reçoit à l'occasion des appels de menaces de la part de personnes en colère. Si des menaces sont proférées à l'endroit de membres du personnel, la procédure suivante doit être respectée :

1) L'employé au téléphone qui reçoit les menaces à l'endroit d'un autre employé devrait prendre soin d'écrire le nom de la personne qui profère les menaces et noter le numéro de téléphone duquel appelle la personne. Il devrait aussi confirmer l'endroit où se trouve l'interlocuteur et noter autant de détails que possible tirés de la conversation.
2) L'employé devrait ensuite aviser immédiatement son gestionnaire, le SSU et les Services juridiques en indiquant tous les détails ci-dessus.
3) Dans ces situations, le SSU prend le contrôle, conjointement avec les Services juridiques, le directeur des Services corporatifs, le directeur général des Opérations et l'Ombudsman.
4) Tous les membres du personnel seront informés de la menace potentielle à la sécurité et recevront des instructions précises si on croit qu'il y a un risque pour le personnel.
5) Le SSU s'occupera d'escorter la police et les autres professionnels de la sécurité au besoin. Il sera l'agent de liaison principal auprès des services de sécurité du bâtiment.

3.20.3 Bouclage de la réception

Quand des menaces sont proférées, le SSU peut décider de boucler l'aire de réception. Ce secteur doit être inclus dans le bouclage, même s'il n'est plus utilisé. Il demeure un point d'accès aux bureaux.

3.20.4 Plaintes en personne

Le Bureau reçoit parfois des plaignants sur place. Habituellement, ces cas sont pris en charge par les agents d'accueil. Toutes les plaintes en personne doivent être reçues dans la salle d'entrevue, idéalement par deux employés. Les employés ne doivent pas entendre seuls les plaintes en personne. Dans les cas où le plaignant devient agressif, menaçant ou représente un quelconque danger pour le Bureau, on doit lui demander de partir et signaler l'incident au SSU immédiatement. Ne suivez

pas la personne jusqu'à la sortie du bâtiment. Après que vous aurez avisé le SSU, les commissionnaires du bâtiment seront avisés et s'assureront que la personne quitte les lieux. Si la personne refuse de partir, vous pouvez quitter la pièce et demander l'aide du SSU (quand les deux portes sont fermées, la personne ne peut quitter la pièce sans une carte d'accès) ou, si vous croyez être en danger, utilisez le bouton d'alarme pour alerter les autorités.

3.20.5 Courrier ou colis suspects

La menace principale que représentent le courrier et les colis est l'exposition aux agents radioactifs, explosif, biologique ou chimique.

Un colis suspect consiste en un colis ou une enveloppe que l'on trouve ou reçoit et qui soulève des soupçons de la part du particulier que le reçoit ou est chargé de sa manipulation. Le colis peut arriver par courrier ordinaire, envoi spécial, services de messagerie ou livraison personnelle. Parfois il aura été précédé de lettres, d'appels téléphoniques ou d'avis dans lesquels on aura proféré des menaces. Chaque type d'objet suspect pose un risque différent et il n'y a pas une façon générale de le gérer.

S'il est question de courrier ou de colis suspects, il faut avant tout tenir compte de la santé et de la sécurité des occupants de l'immeuble. Le *Code canadien du travail* et d'autres lois et règlements obligent l'employeur et d'autres personnes responsables des conditions d'occupation dans les immeubles à établir un plan d'urgence et à faire preuve de « diligence raisonnable » afin de réduire les dangers et les risques dans le milieu de travail. Par conséquent, toutes les précautions possibles doivent être prises. Dans le doute, mieux vaut être trop prudent.

3.20.6 Substances ou objets suspects

Les substances ou objets suspects pourraient comprendre un déversement chimique, des fumées toxiques, une substance biologique ou radioactive.

- **NE PAS TOUCHER** l'objet suspect;
- Informer le gestionnaire compétent et le SSU;
- Informer le service d'incendie et l'organisme des mesures d'urgence de l'immeuble;
- Préserver l'intégrité des lieux;
    - Éloigner le personnel de la substance ou de l'objet,
    - Si possible, isoler ou couvrir la substance ou l'objet.

Voir l'annexe F pour plus d'information à ce sujet.

3.20.7 Alertes à la bombe

L'origine d'une alerte à la bombe peut varier : l'alerte peut être exprimée en personne, par appel téléphonique ou par écrit (y compris par courriel, médias sociaux (Facebook, Twitter) et le Live Chat.).

Alerte à la bombe par appel téléphonique

- Écouter attentivement, être poli et permettre à l'interlocuteur de s'exprimer le plus possible sans interruption;
- Demander et noter, si possible : l'heure à laquelle la bombe doit éclater? l'emplacement de la bombe? à quoi ressemble la bombe? de quel endroit l'interlocuteur appelle-t-il? où la bombe a-t-elle été placée? quel est le nom de l'interlocuteur?
- Consigner la date, l'heure, la durée de l'appel et la formulation exacte de la menace;
- Déterminer les traits personnels : sexe, accent, voix (forte, douce), débit (rapide, lent), prononciation, manières;
- Retenir l'information sur l'AFFICHEUR de l'appareil téléphonique, si disponible;
- Informer le gestionnaire compétent et/ou le SSU;
- Le gestionnaire et/ou le SSU informe la police et l'organisme chargé des mesures d'urgence pour le bâtiment;
- Remplir l'annexe E – Liste de vérification (menaces par appel téléphonique).

Alerte à la bombe en personne

- Ne pas antagoniser l'individu ou les individus;
- Suivre les instructions et être vigilant;
- Éviter de sembler hostile;
- Ne pas parler à moins d'être appelé à le faire;
- Préserver l'intégrité des lieux s'il n'y a pas de danger pour soi;
- Informer le gestionnaire compétent et/ou le SSU;
- Le gestionnaire ou le SSU informe la police.

Si l'on soupçonne une bombe

- **NE PAS TOUCHER** l'objet suspect;
- Informer le gestionnaire compétent et le SSU;
- Informer la police (NE PAS UTILISER le RADIOTÉLÉPHONE ou le TÉLÉPHONE CELLULAIRE);
- Préserver l'intégrité des lieux;
- Éloigner le personnel de l'objet.

3.20.8 Lettres ou appels menaçants ou malveillants

Appels téléphoniques

- Écouter attentivement, être poli et permettre à l'interlocuteur de s'exprimer le plus possible sans interruption;
- Consigner la date, l'heure, la durée de l'appel et la formulation exacte de la menace;
- Déterminer les qualités personnelles : sexe, accent, voix (forte, douce), débit (rapide, lent), prononciation, manières;
- Retenir l'information sur l'AFFICHEUR de l'appareil téléphonique, si disponible;
- Informer le gestionnaire compétent et/ou le SSU;
- Le gestionnaire ou le SSU informe la police.

Lettres

- Éviter de manipuler l'objet excessivement;
- Conserver tout matériel comme éléments de preuve;
- Informer le gestionnaire compétent et/ou le SSU;
- Le gestionnaire ou le SSU informe la police.

Courriel

- Ne pas supprimer le courriel;
- Informer le gestionnaire compétent et/ou le SSU;
- Le gestionnaire ou le SSU informe la police.

Message dans la boîte vocale

- Ne pas supprimer le message;

- Informer le gestionnaire compétent et/ou le SSU;
- Le gestionnaire ou le SSU informe la police.

Annexe A – Tableau sommaire – Renseignements classifiés ou désignés

Tableau sommaire

NIVEAU/ MARQUAGE	**PORTÉE DU PRÉJUDICE À L'INTÉRÊT NATIONAL**	**PORTÉE DU PRÉJUDICE À D'AUTRES INTÉRÊTS**
TRÈS SECRET	Exceptionnellement grave	
SECRET	Grave	
CONFIDENTIEL	Limitée	
PROTÉGÉ C		Exceptionnellement grave
PROTÉGÉ B		Grave
PROTÉGÉ A		Limitée

Annexe B – Formulaire de réunion

Ombudsman

National Defence and Canadian Forces | Défense nationale et Forces canadiennes

MEETING / RÉUNION

Date / Date :

Time / Heure :

Floor / Étage : th Floor / e étage

Contact Person / Personne responsable :

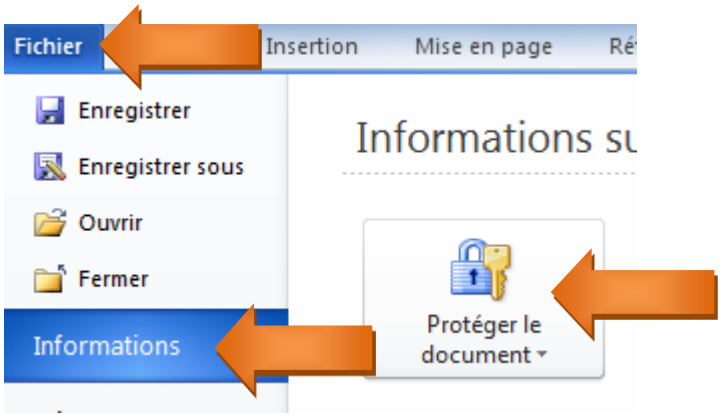
Telephone Number / Numéro de téléphone :

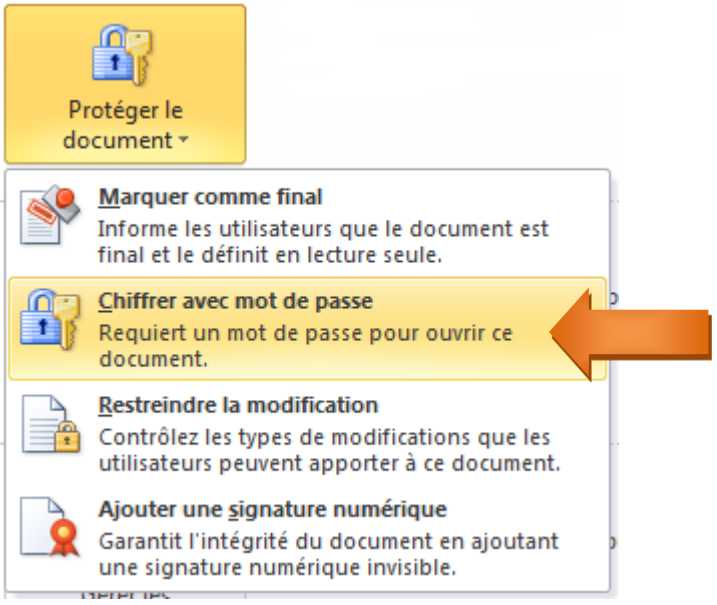
Attendees / Participants	Department or Agency / Ministère ou organisme

Annexe C – Protection de documents par mot de passe

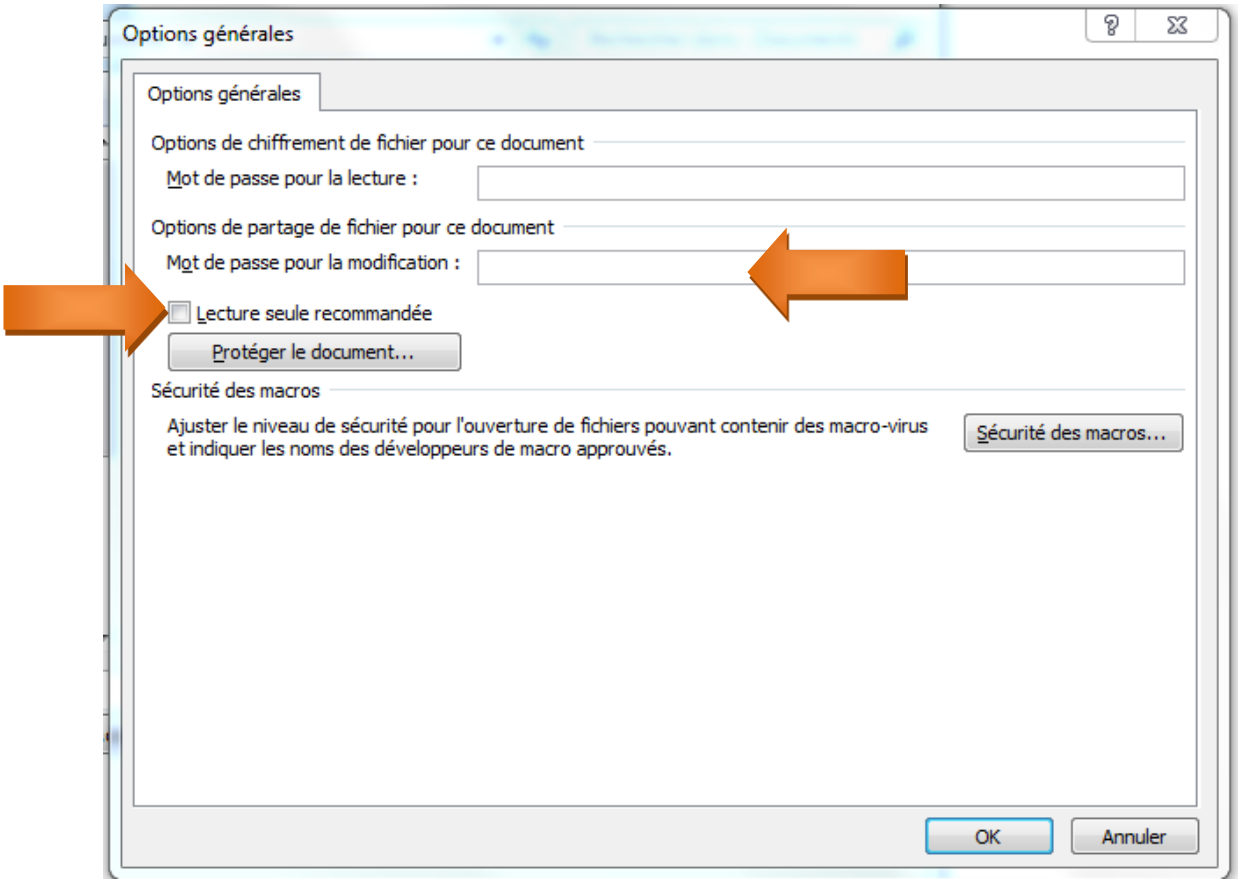
Dans Microsoft Word 2010

Cliquez sur Fichier / Informations / Protéger le document / Chiffrer avec mot de passe. Vous pouvez demander un mot de passe pour ouvrir ou modifier ou choisir « Lecture seule recommandée ». Vous pouvez utiliser les trois options ensemble ou choisir n'importe quelle combinaison.





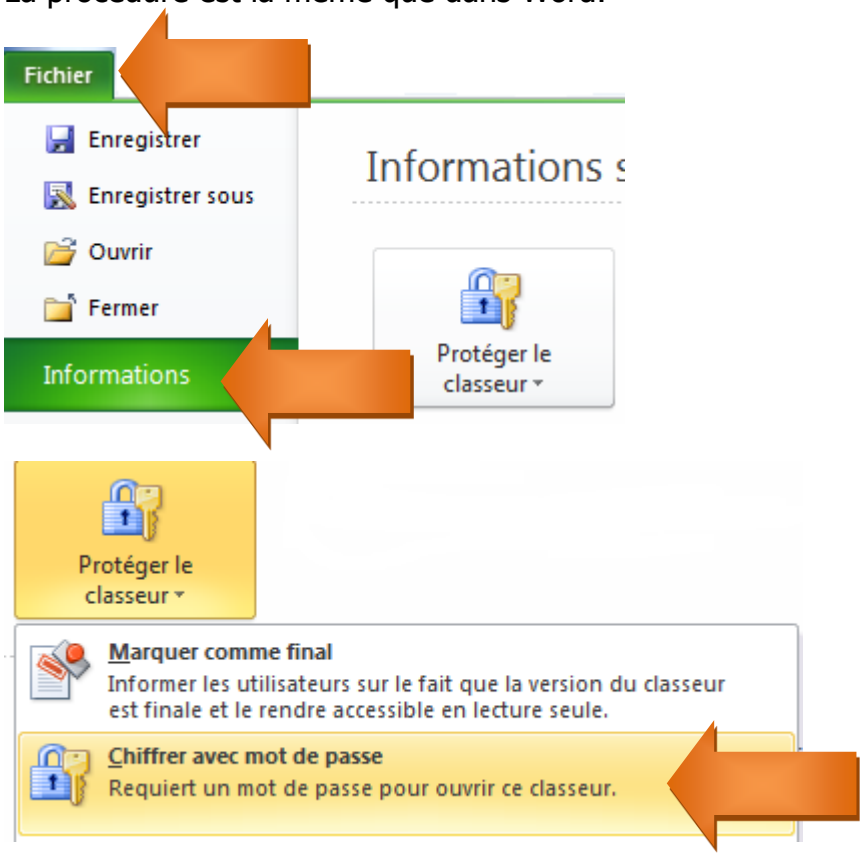
Un document Word peut aussi être protégé quand il est partagé à grande échelle. Pour utiliser ce type de protection, cliquez sur Fichier / Enregistrer sous / Parcourir. Dans le coin inférieur droit, cliquez sur Outils, puis Options générales. Une fenêtre s'ouvrira.



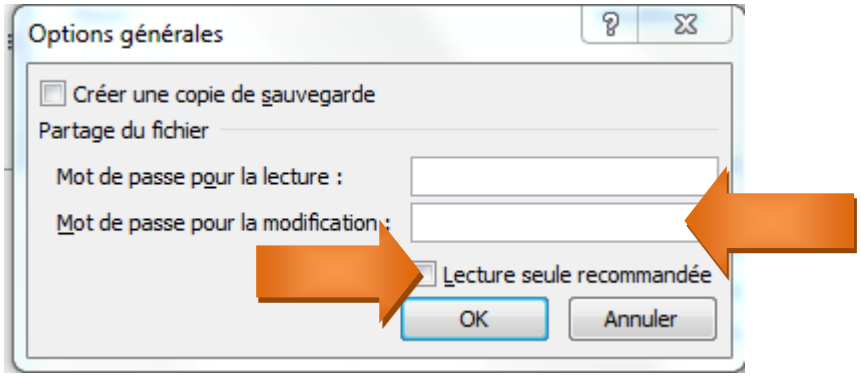
Cliquez sur OK à la fin.

Dans Microsoft Excel 2010

Cliquez sur Fichier / Informations / Protéger le classeur / Chiffrer avec mot de passe. La procédure est la même que dans Word.



Un document Excel peut aussi être protégé quand on le partage à grande échelle. Pour utiliser ce type de protection, cliquez sur Fichier / Enregistrer sous / Parcourir. Dans le coin inférieur droit, cliquez sur Outils / Options générales. Une fenêtre s'ouvrira.



Cliquez sur OK à la fin.

Annexe D – Balayage de clés USB, de CD, de DVD, etc.

1) Brancher ou insérer le support
2) Ouvrir l'explorateur de fichiers et cliquer sur Ordinateur, clic droit sur l'icône du support à balayer, Rechercher les menaces.
3) Une fenêtre s'ouvre. Le système effectue le balayage et informe l'utilisateur lorsque le processus est terminé. Permettre l'exécution du balayage avant d'ouvrir un document sauvegardé sur le support.

Annexe E – Liste de vérification (menaces par appel téléphonique)

Questions à poser :

À quelle heure la bombe doit-elle éclater? (alerte à la bombe) Que se passera-t-il? (autres menaces)
Où est la bombe ou l'objet?
À quoi ressemble la bombe ou l'objet?
De quel endroit appelez-vous?
Pourquoi a-t-on placé la bombe ou l'objet?
Quel est votre nom?

Déterminer les qualités personnelles de l'interlocuteur :

Sexe :	Homme	Femme	Incertain	
Âge approximatif (préciser) :				
Accent :	anglais	français	autre	
Voix :	forte	douce	autre	
Débit :	rapide	lent	autre	
Prononciation :	bonne	nasillarde	zézayée	autre
Manières :	émotif	calme	vulgaire	autre
Bruit de fond : (préciser)				
La voix est familière : (préciser)				
L'interlocuteur semble connaître les lieux : (préciser)				

FORMULATION EXACTE DE LA MENACE :

_____

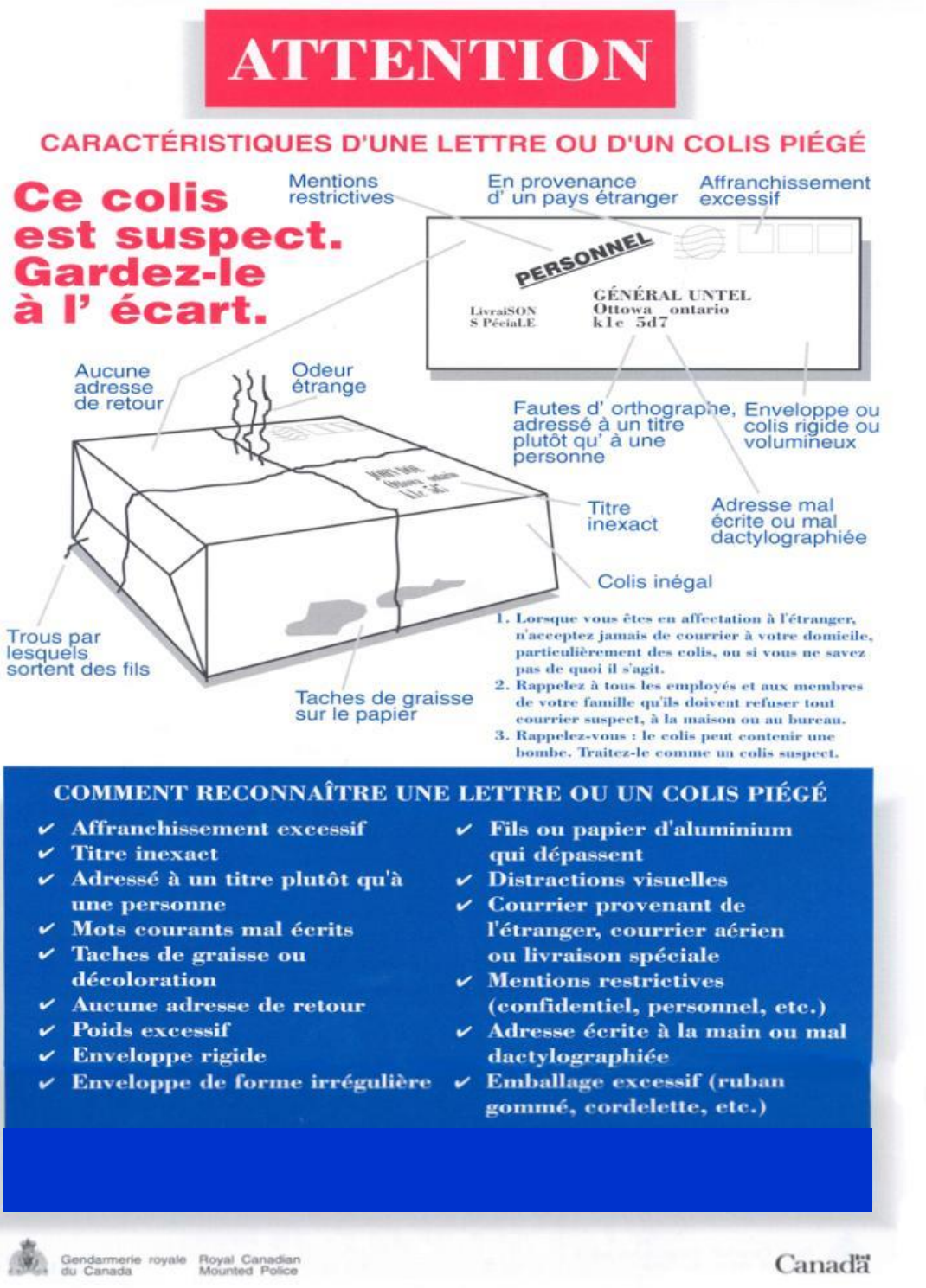
_____

_____

Date : _____ Heure : _____

Durée de l'appel : _____

Annexe F – Alerte à la bombe



Annexe G – Guide de référence relatif aux documents

	Protégé A	**Protégé B**	**Protégé C**	**Confidentiel**	**Secret**	**Très secret**
Cote de sécurité	Fiabilité de base	Fiabilité de base	Fiabilité de base	Cote Confidentiel (Niveau l)	Cote Secret (Niveau ll)	Cote Très secret (Niveau lll)
Marquage	Angle supérieur droit si l'envoi est à l'extérieur du Bureau (Voir Envoi de courrier)	Angle supérieur droit de chaque page	Angle supérieur droit de chaque page	Angle supérieur droit de chaque page	Angle supérieur droit de chaque page	Angle supérieur droit de chaque page
Entreposage de documents papier	Bureau verrouillé ou coffre avec cadenas à clé	Armoire de sécurité approuvée avec serrure à combinaison ou cadenas à clé approuvé	Armoire de sécurité approuvée pour documents Protégé C - conforme au *Guide de l'équipement de sécurité*	Armoire de sécurité approuvée pour documents Confidentiels - conforme au *Guide de l'équipement de sécurité*	Armoire de sécurité approuvée pour documents Secret - conforme au *Guide de l'équipement de sécurité*	Armoire de sécurité approuvée et avec combinaison intégrée pour documents Très secret - conforme au *Guide de l'équipement de sécurité*
Entreposage de supports électroniques	Lecteurs et dossiers partagés du Bureau; supports portatifs (CD, disquettes, clés USB) étiquetés et à accès limité	Lecteurs et dossiers partagés du Bureau; supports portatifs (CD, disquettes, clés USB), étiquetés, à accès limité et protégés par mots de passe	Supports portatifs (CD, disquettes, clés USB), étiquetés, verrouillés à l'instar des documents papier entreposés, et protégés par mots de passe	Supports portatifs (CD, disquettes, clés USB), étiquetés, verrouillés à l'instar des documents papier entreposés, et protégés par mots de passe	Supports portatifs (CD, disquettes, clés USB), étiquetés, verrouillés à l'instar des documents papier entreposés, et protégés par mots de passe	Supports portatifs (CD, disquettes, clés USB), étiquetés, verrouillés à l'instar des documents papier entreposés, et protégés par mots de passe
Transmission électronique	Réseau interne du Bureau – système A ou B	Réseau interne du Bureau - ICP	Aucune transmission électronique	Réseau interne du Bureau - ICP	Aucune transmission électronique	Aucune transmission électronique
Télécopieur	Télécopieur ordinaire	Télécopieur ordinaire	Aucun télécopieur	Aucun télécopieur	Aucun télécopieur	Aucun télécopieur

	Protégé A	Protégé B	Protégé C	Confidentiel	Secret	Très secret
Téléphone	Ligne RL (téléphone ordinaire)	Ligne RL (téléphone ordinaire)	STU III – Voir SSU	Ligne RL (téléphone ordinaire)	STU III – Voir SSU	STU III – Voir SSU
Destruction	Machine à détruire les documents	Machine à détruire les documents	Machine à détruire les documents	Machine à détruire les documents	Machine à détruire les documents	Machine à détruire les documents
Emballage	1 enveloppe collée ou 1 boîte scellée simple, aucune marque de sécurité (une enveloppe réutilisable ou une chemise étiquetée suffit pour livraison à l'intérieur du Bureau)	1 enveloppe collée ou 1 boîte scellée simple, aucune marque de sécurité (une enveloppe réutilisable ou une chemise étiquetée suffit pour livraison à l'intérieur du Bureau)	2 enveloppes collées; colis encombrant ou lourd enveloppé de deux épaisseurs scellées; mettre l'adresse sur les deux épaisseurs; marquer l'épaisseur intérieure de « Ne doit être ouvert que par »; inscrire l'envoi dans le registre des envois	À l'exception des envois à l'étranger (voir ci-dessous), 1 enveloppe collée ou 1 boîte scellée simple, aucune marque de sécurité (une enveloppe réutilisable ou une chemise étiquetée suffit pour livraison à l'intérieur du Bureau)	À l'exception des envois à l'étranger (voir ci-dessous), 1 enveloppe collée ou 1 boîte scellée simple, aucune marque de sécurité (une enveloppe réutilisable ou une chemise étiquetée suffit pour livraison à l'intérieur du Bureau)	2 enveloppes collées; colis encombrant ou lourd enveloppé de deux épaisseurs scellées; mettre l'adresse sur les deux épaisseurs; marquer l'épaisseur intérieure de « Ne doit être ouvert que par »; inscrire l'envoi dans le registre des envois
Livraison interne	Par courrier interne	Par courrier interne	Dans une enveloppe scellée, livraison par porteur	Livraison interne dans une enveloppe scellée	Livraison interne dans une enveloppe scellée	Dans une enveloppe scellée, livraison par porteur
Envoi par courrier	Dans la RCN courrier de 1re classe Autres villes du Canada courrier de 1re classe À l'étranger Par courrier de 1re classe ou, en cas d'urgence,	Dans la RCN courrier de 1re classe Autres villes du Canada courrier de 1re classe À l'étranger Par courrier de 1re classe ou, en cas d'urgence, par services de	Dans la RCN Services de messagerie détenant la cote Très secret; dans une mallette de sécurité verrouillée pour passer d'un immeuble à un autre Autres villes	Dans la RCN Services de messagerie détenant la cote Confidentiel; dans une mallette de sécurité pour passer d'un immeuble à un autre Courrier de 1re classe, dans deux	Dans la RCN Services de messagerie détenant la cote Secret; dans une mallette de sécurité pour passer d'un immeuble à un autre Courrier de 1re classe, dans deux enveloppes	Dans la RCN Services de messagerie détenant la cote Très secret; dans une mallette de sécurité verrouillée pour passer d'un immeuble à un autre Autres villes du Canada

	Protégé A	**Protégé B**	**Protégé C**	**Confidentiel**	**Secret**	**Très secret**
	par services de messagerie commerciale fiables	messagerie commerciale fiables	du Canada Par courrier recommandé À l'étranger Services d'envoi diplomatique de sécurité; mettre l'adresse Division de la distribution (SBG) MAECI sur l'enveloppe extérieure; le destinataire et le marquage de sécurité ne doivent figurer que sur l'enveloppe intérieure; insérer entre les deux enveloppes le formulaire GC 44 « Note d'envoi et reçu »; sceller l'enveloppe intérieure (ou le papier d'emballage intérieur) avec du ruban inviolable	enveloppes dont l'enveloppe intérieure est marquée de « Ne doit être ouvert que par »; envoi inscrit dans le registre des envois Autres villes du Canada Confidentiel – courrier de 1re classe et enregistrement du transit et de la livraison, ou services de messagerie commerciale fiables À l'étranger Emballage et livraison semblable à celles des documents Très secret	dont l'enveloppe intérieure est marquée de « Ne doit être ouvert que par »; envoi inscrit dans le registre des envois Autres villes du Canada Secret – services de messagerie fiables et enregistrement du transit et de la livraison À l'étranger Emballage et livraison semblable à celles des documents Très secret	Par courrier recommandé À l'étranger Services d'envoi diplomatique de sécurité; mettre l'adresse Division de la distribution (SBG) MAECI sur l'enveloppe extérieure; le destinataire et le marquage de sécurité ne doivent figurer que sur l'enveloppe intérieure; insérer entre les deux enveloppes le formulaire GC 44 « Note d'envoi et reçu »; sceller l'enveloppe intérieure (ou le papier d'emballage intérieur) avec du ruban inviolable
Livraison par porteur	Dans une mallette	Dans une mallette	Dans une mallette	Dans une mallette	Dans une mallette	Dans une mallette

	Protégé A	**Protégé B**	**Protégé C**	**Confidentiel**	**Secret**	**Très secret**
	étiquetée de l'adresse de retour du Bureau	étiquetée de l'adresse de retour du Bureau	approuvée étiquetée de l'adresse de retour du Bureau	approuvée étiquetée de l'adresse de retour du Bureau	approuvée étiquetée de l'adresse de retour du Bureau	approuvée étiquetée de l'adresse de retour du Bureau

Annexe H – Procédure d'appel nominal

Il est nécessaire pour le Bureau de l'Ombudsman de mettre en place un moyen pour faire le compte des employés lors d'une évacuation.

Au déclenchement d'une crise, les employés, clients et invités doivent quitter les lieux. Quand cela se produit, la plupart du temps, nous nous retrouvons séparés de nos collègues. La procédure suivante a été adoptée par le Bureau de l'Ombudsman pour s'assurer que toutes les personnes dont nous sommes responsables ont pu quitter le bâtiment sans encombre.

Procédure

1. En sortant du bâtiment, rendez-vous immédiatement au World Exchange Plaza situé à l'intersection des rues Metcalfe et Albert, un coin de rue au nord de notre bâtiment (100, rue Metcalfe). Il y a plusieurs entrées au World Exchange Plaza, mais nous vous recommandons d'utiliser l'entrée Metcalfe.

2. Une fois que vous êtes dans le World Exchange Plaza, localisez la personne qui porte une veste de construction jaune hautement visible. Cette personne sera dans la zone de l'entrée Metcalfe. Vous devez signaler votre présence à cette personne. En même temps, les gestionnaires se rassembleront dans les environs pour vérifier toute absence parmi les membres de leur équipe, rencontrer les employés et donner à ceux-ci des nouvelles et des consignes.

3. Il revient à chaque employé de suivre ces étapes en cas d'évacuation réelle ou d'exercice.

Annexe I – Vérifications de sécurité

Comme on l'indique à la section 3.15 du Manuel de sécurité, tous les employés du Bureau de l'Ombudsman peuvent subir des vérifications de sécurité.

Le superviseur de la sécurité de l'unité ou un gestionnaire désigné peut procéder à des vérifications aléatoires après les heures de bureau. Aucun avis ne sera émis avant une vérification.

Des vérifications ponctuelles peuvent être menées pendant les heures de bureau si des informations reçues le justifient. La politique de bureau propre mentionné à la section 3.6.1 devrait être appliquée durant les heures de bureau.

Lors des vérifications en dehors des heures ouvrables, les responsables vérifieront notamment ce qui suit :

- Information de nature délicate mal entreposée;
- Classeurs non verrouillés;
- Ordinateurs dont la session n'a pas été fermée;
- Documents déchiquetés laissés à la vue,
- Documents classifiés ou Protégé B jetés dans le bac à recyclage;
- Clés mal entreposées (ex. cachées dans les murs du poste de travail ou dans un porte-crayon);
- Courrier sortant laissé dans la corbeille à cet effet;
- **Objets attrayants laissés à la vue, p. ex. BlackBerry, enregistreurs numériques, ordinateurs portables, clés USB, cartes ICP, etc.**

Les documents laissés sur les imprimantes Protégé B seront déchiquetés.

Une porte de bureau fermée est un moyen acceptable pour ranger temporairement les documents Protégé B ou d'une désignation inférieure pendant les heures ouvrables. Lors des inspections en dehors des heures ouvrables, on vérifiera si les portes sont verrouillées. Les bureaux non verrouillés seront susceptibles d'être examinés au même titre que les poste de travail. Une porte fermée ne peut remplacer un classeur approuvé.

Les vérifications de sécurité effectuées seront de nature visuelle. On inspectera visuellement les alvéoles et bureaux, à la recherche d'infractions. On vérifiera la présence de clés dans les porte-crayons et à trombones et sur les panneaux des postes de travail. **Nous ne tolérons pas les clés cachées. En fait, les clés ne devraient jamais être cachées. Elles devraient être rangées en sûreté ou en la possession de leur propriétaire.** On inspectera les bacs à recyclage à la recherche de documents classifiés. Les caissons à tiroir seront ouverts seulement s'ils sont laissés déverrouillés. Il faut bien comprendre que tous les dossiers doivent

être rangés dans des classeurs approuvés. Veuillez noter que les armoires supérieures et les caissons à tiroir ne sont pas des unités de rangement approuvées pour les documents classifiés ou désignés.

Annexe J – Blocs de signature normalisés

Les consignes suivantes sont obligatoires en vertu de l'annexe E : Blocs-signatures du courriel. Veuillez noter que la politique du Bureau et les cas laissés à la discrétion des utilisateurs sont décrits ci-dessous.

Exigences obligatoires

La normalisation des sites Internet exige que le programme de coordination de l'image de marque et la politique sur les langues officielles soient respectés.

- Le texte doit être de couleur noire sur fond blanc.
- Les polices suivantes sont acceptables : styles de police sans-sérif, comme Verdana, Calibri ou Arial
- Taille de la police : 10 points.
- La signature doit être en caractères d'imprimerie, et non en lettre cursives, afin d'être lisible par les handicapés visuels.
- Tous les courriels envoyés par des employés du gouvernement à des destinataires qui ne font pas partie du gouvernement du Canada doivent inclure un bloc signature dans les deux langues officielles.
- Pour employés dont le bureau est situé à l'extérieur du Québec, l'anglais doit précéder le français dans le bloc de signature, et vice-versa pour les employés situés au Québec.
- Tous les courriels envoyés par les employés du gouvernement du Canada doivent comprendre les renseignements suivants : nom de l'auteur, institution, numéro de téléphone, numéros sans frais et ATS (avec l'indicatif régional).
- Le bloc de signature doit être sur la même page que la fin du message (et non dans un fichier ou une pièce jointe distincte).
- Tous les courriels doivent comprendre la mention « Government of Canada/ Gouvernement du Canada ».
- Les mêmes exigences s'appliquent pour les courriels envoyés sur les appareils mobiles, si la technologie le permet.
- Ne pas ajouter d'adresse de bâtiment aux blocs de signature.

Politique du Bureau :

- Le personnel des Opérations doit indiquer le numéro principal (613-992-0787) et le numéro sans frais (1-888-828-3626) du Bureau dans le bloc de signature.
- Les images et photographies (p. ex. visages-sourires, émoticônes, symboles, etc.) ou les logos d'associations ou d'organisations auxquelles l'employé appartient (ou a déjà appartenu) ne sont pas permis.
- Les adages, citations, extraits de poèmes ou bannières sont interdits dans les blocs de signature.

- Les blocs de signature doivent comprendre un court avertissement après la signature (voir l'exemple à la fin du présent document).

Cas laissés à la discrétion des employés :

- Il faut garder à l'esprit notre position unique au sein du gouvernement et notre indépendance vis-à-vis du MDN et des FAC. Plus particulièrement, nous devons être conscients des perceptions possibles en ce qui concerne nos clients et leurs attentes légitimes en matière d'impartialité. Pour cette raison, le Bureau demande à ses employés de ne pas indiquer, dans leur bloc de signature, leur ancien grade militaire (le cas échéant), les décorations reçues (ex. Décoration des Forces canadiennes – CD) ou leur appartenance à des associations professionnelles.
- Les capacités et accomplissements liés aux études postsecondaires sont reconnus par le Bureau, mais les abréviations de diplôme/certificat après le nom d'une personne peuvent parfois mener à confusion (surtout si le diplôme obtenu n'est pas lié au travail effectué). L'inclusion des honneurs liés aux études dans les blocs de signatures, même si elle n'est pas encouragée, est laissée à la discrétion de chacun.
- Un hyperlien menant au site Web du Bureau peut être ajouté au bloc de signature s'il s'agit d'un programme ou d'un service offert. Utilisez le lien universel (http://www.ombudsman.forces.gc.ca). Le bloc de signature générique est présenté dans le même format que celui de la personne, sauf qu'au lieu du nom de la personne, on indique le titre du programme ou service.
- Veuillez demander l'aide de votre directeur si vous rencontrez des problèmes techniques pour créer ou modifier le bloc de signature dans votre boîte de courriels.

Modèle de signature :

John Smith

Investigator, Investigations, Office of the Ombudsman
Department of National Defence / Government of Canada
John.Smith@forces.gc.ca / Tel: 613-992-0787 / Toll Free: 1-888-828-3626

Enquêteur, Enquêtes, Bureau de l'Ombudsman
Ministère de la Défense nationale / Gouvernement du Canada
John.Smith@forces.gc.ca / Tél : 613-992-0787 / Sans Frais : 1-888-828-3626

If you have received this message in error, please delete it and notify me.
Si vous avez reçu ce courriel par erreur, veuillez le supprimer et m'en aviser.

Glossaire

Voici un glossaire des sigles utilisés dans le présent document.

CIDP	code d'identification de dossier personnel
DG	directeur général
FC	Forces canadiennes
GRC	Gendarmerie royale du Canada
ICP	infrastructure à clés publiques
MDN	ministère de la Défense nationale
PPA	Plan de poursuite des activités
PM	police militaire
PCIM	Programme de coordination de l'image de marque
RCN	Région de la capitale nationale
SCT	Secrétariat du Conseil du Trésor
SPAC	Services publics et Approvisionnement Canada
SSU	Surveillant de la sécurité de l'unité