Ombudsman
National Defence and Canadian Armed Forces

Security Handbook

2017

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

Table of Contents

1 Introduction

The following security handbook has been designed to assist the employees of the Office of the Ombudsman in fulfilling individual security responsibilities involved in the day-to-day work in support of the Mandate. As a federal government office, there is a requirement for all employees, under the Government Security Policy, to protect the assets (information and technology) in the Office's possession.

This handbook provides guidelines on the classification of documents, security markings, mailing, handling, storing, transmitting and transportation of documentation as well as many other security-related subjects of interest to the employees of the Office of the Ombudsman. It also provides internet links to sites where further information and policies can be found.

If, at any time, you wish to discuss security requirements further please do not hesitate to talk to your responsible manager, the Unit Security Supervisor, or the Legal Services group.

Gary Walbourne

Ombudsman

1.1 Updates

Area Changed	Changes Made
Table of Contents	New logo added
3.1 Classification of Documents	3.1.1 Introduction: added links to the Access to Information Act and the Privacy Act for more information regarding both.
	3.1.2 Classified/Protected Information: Updated links for policy on government security and security information (National Defence Security Orders and Directives). Added hyperlink to Annex A
3.2 Marking	Reference to PKI (hyperlink added)
	Added link to internal IM Policies
3.3 Access	3.3.1 Document Access: Updated link to Security Equipment Guide
	3.3.2 Access Zones: Reception area is now an access point only to the office.
	3.3.3 ID Cards/Passes: Removed mention of the NDI 80 NCR pass. Added link to DND's Security Directive Number 7. Temporary passes included.
	3.3.4 Visitors: Removed mention of Reception area. Added Commissionaires in regards to sign in. Added link to Policy on Government Security and National Defence Security Policy. Added hyperlink to Annex B and link to actual Form in o:drive.
3.4 Security Screening	3.4.1 Reliability Status and Security Clearances: Update made to reliability check. Mention of Human Resources removed. Updated link to Standard on Security Screening.
	3.4.3 Denial: Updated link to Standard on Security Screening.
	3.4.5 Transfers/Reinstatements: Added hyperlinks to security forms 330-23 and 330-60
3.8 Destruction	Link to internal SOPs added.
3.9 Telephones	Ban on Bluetooth device with cellphone removed.

3.10 Fax	Removed mention and link to fax cover page as it is no longer in use. Removed mention of secure fax as it is no longer in service.
3.11 Laptops and Office Computers	Removed mention of the TEMPEST station as it is no longer in service.
3.13 Desktop Computers	3.13.2 Passwords: added hyperlink to Annex C Added information on passwords in general
	3.13.3 Network Account Briefings: Added link to DAOD 6002-2
	3.13.4 Email: Added hyperlink to Annex J
3.14 USB Sticks/CD/DVD	Added hyperlink to Annex D Added mention of personal phones and tablets
3.16 Security Infractions	Added hyperlink to Annex I
3.19 Physical Security	3.19.1 Panic Buttons: Updated to include strobe lighting.
	3.19.2 Security Alert Level program: Added hyperlinks to sections 3.20.2 Threats
3.20 Emergency Procedures	3.20.1 Emergency Procedures: Added link to Annex H and added link to Small Appliance Policy.
	3.20.6 Suspicious Objects/Substances: Added hyperlink to Annex F.
	3.20.7 Bomb Threats: Added hyperlink to Annex E Added social media and Live Chat
	3.20.8 Threatening/Crank Calls and Letters in the security handbook. Added hyperlink to Annex F.
Annex B: Meeting Form	New logo added.
	Removed reception contact information.
Annex C: How to Password Protect Documents	Updated to reflect our current version of word and excel.
	New screenshots added.
Annex D: How to Scan USB Drives/CDs/DVDs	Updated process on how to accomplish this.
	Removed mention of diskettes.
Annex F (Old): Anthrax	Removed from handbook completely.
Annex F (New): Bomb Threat Poster	Clearer image added.

Annex H: Roll-Call Procedures	Removed reference to reception.
Annex I: Security Checks	Added hyperlinks to section 3.15 and 3.5.1 in the security handbook.
Annex J: Standardized Signature Blocks	Added hyperlink to Appendix E: Email Signature Blocks.
	Updated some of the requirements and the sample signature.
Glossary of Terms	Glossary added.

2 Corporate Responsibilities

In relation to security it is the responsibility of this Office to:

- Protect the information and the assets within our possession;
- Preserve the confidentiality, integrity and value of that information;
- Comply with the requirements of the Ministerial Directives and the Government Security Policy;
- Protect employees from work-related threats; and
- Assure the continued delivery of services, Business Continuity Planning.

2.1 Managers

Managers are responsible to:

- Ensure that individuals have the necessary security clearance before they commence work;
- Remain vigilant once the clearance is granted and act on any new information that could put into question an individual's reliability or loyalty;
- Report security incidents without delay and implement appropriate measures to prevent reoccurrence; and
- Ensure implementation of the security measures set out in this document for their respective sections.

2.2 Employees

Employees and other individuals who work for the Office are responsible to:

- Follow the guidelines established in the handbook;
- Safeguard assets in their custody in accordance with this policy; and
- Report, as soon as possible, threats to their safety and other security incidents to their manager and to the Unit Security Supervisor. Please refer to the Security Level Alert Program (section 3.19.2).

2.3 Unit Security Supervisor

The Unit Security Supervisor (USS) has been designated as the security co-ordinator for the Office. The Unit Security Supervisor is responsible to:

- Brief management on security issues;

- Assist individuals with security concerns and questions related to this policy; and
- To ensure the following policy is kept up-to-date, and reflects the current status of the Government Security Policy; and
- Provides updates as well as training and awareness sessions during all staff meetings.

NOTE: In all cases where the USS is not available, the Alternate USS will act as the point of contact.

3 Protection of Information

3.1 Classification of Documents

3.1.1 Introduction

Information, which is likely to be exempted or excluded from access under the *Access to Information Act* or the *Privacy Act*, is considered to be sensitive. It must be categorized as classified or as protected and marked at the appropriate level.

The *Access to Information Act* gives Canadian citizens the right to access information in federal government records.

The Privacy Act provides citizens with the right to access personal information about themselves held by the government and protection of that information against unauthorized use and disclosure.

See the following website for more information on the *Access to Information Act* and *The Privacy Act*.
http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/index-eng.asp

3.1.2 Classified / Protected Information

Classified information relates to the national interest. It concerns the defence and maintenance of the social, political and economic stability of Canada. Below are the categories of classification:

- **Confidential** – Where disclosure could cause injury to the national interest i.e. physical security threat and risk assessments, combat tactics, tactical doctrines, details of a units war establishment.

- **Secret** – Where disclosure could cause serious injury to the national interest i.e. cabinet confidences, details of the CF war establishments, deployment of forces in an operational role, details of crypto equipment.

- **Top Secret** – Where disclosure could cause exceptionally grave injury to the national interest i.e. particulars of cryptanalysis, all electronic warfare and war plans.

Protected information relates to interests other than the national interest such as personal and private interests. Below are the categories of classification:

- **Protected A** – Labeled as low-sensitivity. When the injury that would result from compromise would be minimal (i.e. personal names, home addresses etc.);

- **Protected B** – Labeled as particularly sensitive. When disclosure could cause serious injury outside of the national interest (i.e. medical information; individual's finances, etc.);

- **Protected C** – Labeled as extremely sensitive. When disclosure of this information could cause exceptionally grave injury outside of national interest; (i.e. serious criminal intelligence, loss of life etc.)

Please see Annex A for a Summary table of what has just been detailed.

Please note that Solicitor-Client information must be marked as such and treated as Protected B information.

For more information on the identification of classified and protected information, consult your manager and your Unit Security Supervisor. There are also many sources for more information on this subject that you should explore:

Treasury Board – Policy on Government Security

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

National Defence Security of Instructions – Chapter 6 National Defence Sucurity Orders and Directives

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

3.2 Marking

The writers or originators of documents are responsible to determine whether the documents contain classified and/or protected information. Documents are to be

marked in accordance with the highest level of sensitivity of the information that they contain or that any attachment contains.

The marking must appear in the upper right-hand corner of every page.

Please note that a document, when labeled in terms of security markings, may be either protected or classified but not both; it should be marked as one or the other.

The Security marking Confidential should not be confused with the marking Personal and Confidential - the latter is intended to keep your information personal or between two people (i.e. your leave forms can be considered confidential for your own purposes but are labeled as Protected B for security purposes). Protected C and Top Secret information will very rarely be held by the Office and should only be marked, stored and handled after consultation with the Unit Security Supervisor (USS).

For guidance on how to choose the appropriate marking please consult your manager, Unit Security Supervisor and/or please visit the following website: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12333

Emails should not be used for communicating sensitive information or documents. However, Protected B can be sent over the network if encrypted using Public Key Infrastructure (PKI). Information or documents that contain sensitive information classified above Protected B may not be sent via email even when being encrypted using a PKI card.

In certain cases, assets other than documents may require marking or labeling because of their sensitivity. Some examples include:

- Combinations to security cabinets that contain classified or protected information or valuable assets and;
- Passwords that allow access to systems where sensitive information is stored.

The Unit Security Supervisor is solely responsible for this activity. Please see the IM Policies for more information and guidance.

3.3 Access

3.3.1 Document Access

Access to classified and protected information and other assets must be limited to those individuals who have a "need-to-know" of the information, or are required to

have access to the assets in the performance of their duties, **and** who have the appropriate security screening level.

Information should not be shared with anyone who does not have a "need-to-know" of the information at hand.

You should ensure that the documents in your possession are locked in the appropriate containers. For guidance on the use of appropriate locking containers please see the Unit Security Supervisor or visit the following webpage:
http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm

3.3.2 Access Zones

Access to the occupied areas of the Office is limited to employees and others who are specifically authorized by the responsible Manager and/or Unit Security Supervisor. Non-employees and visitors are to be escorted by an Office employee at all times while inside the Office.

Employees and others who are specifically authorized must challenge individuals whom they do not recognize and who are seeking entry or have already entered the area. Any attempt at unauthorized entry must be immediately reported to the Unit Security Supervisor.

ZONE	Office of the Ombudsman
Reception	At the building entrances, during work hours, security guards, and access card readers control access. Outside of work hours, access is controlled through locked doors, access card readers, and security guard patrols. Reception areas are designated as public areas for the purpose of receiving visitors or deliveries. Access to the Office areas on the 12th and 13th floors are controlled by card readers from the elevator hallways into the Office occupied areas.
Operations	Includes working areas that are past the reception zones and before entering security zones. Access is controlled through the reception zones and is limited to persons with an access card and, during work hours, to authorized visitors under escort. These areas form the bulk of the space occupied by the Office and where Protected "A", Protected "B" and Confidential information is processed and stored.

Security	These areas are normally enclosed. Examples include the records storage area and the IT server room. During work hours, access is tightly controlled. Access is limited to people who work in the area, and during work hours, to authorized visitors under escort. Access after-hours is not permitted to non-authorized individuals.

3.3.3 ID Cards/Passes

National Defence Headquarters

Individuals, who work at the Office of the Ombudsman, are issued an identification card and/or building pass by National Defence Headquarters (based on their employment status) that they must show on request to the building security guards or other individuals at facilities being visited. In order to gain access to specific DND buildings, pass holders must swipe their card and enter a PIN.

- Indeterminate employees – receive an NCR building pass and an NDI 21 identification card.
- All other individuals – receive an NCR building pass or an Ombudsman pass only.

Indeterminate employees can use their NDI 21 card to sign in to any DND building within the NCR if they are required to visit another location. Individuals may be asked anytime to show their NDI 21 card while circulating in DND buildings; therefore, it should be carried at all times.

Urbandale

Electronic access card readers are used to control access during and/or outside of normal work hours. The Unit Security Supervisor issues access cards to this system. Electronic access card are not to be shared or loaned.

Individuals must take reasonable precautions to safeguard any card issued to them from loss, theft or use by any other person. The loss or theft of a card must be reported immediately to the Unit Security Supervisor. Upon leaving employment at the Office, cards must be returned to the Unit Security Supervisor.

Temporary passes for service personnel and contractors to access the Office during work hours are available from the Unit Security Supervisor. An assessment will be made whether the individual will require escorting or will be provided an access pass. For access outside of work hours, the Unit Security Supervisor must be

contacted. Access passes issued to non-employees are to be strictly controlled and monitored. The access pass is to be retrieved upon termination of the access requirements.

Temporary passes are available from the Unit Security Supervisor if an individual forgets his or her pass. These passes must be returned within 24 hours.

Damaged / broken passes can be replaced by contacting the Unit Security Supervisor.

See DND's Security Directive number 7 for more information concerning DND issued passes.

3.3.4 Visitors

Visitors must report to the commissionaire's desk in the main lobby. Upon confirmation of their appointment, all visitors will be issued a visitor card and will be signed into a logbook held by the commissionaires. All visitors must be escorted to and from the main lobby. The person being visited is responsible for providing the escort. Once admitted, all visitors become the responsibility of the persons authorizing the visits.

Visitor sign in is a common practice throughout the government. Within DND you are required to sign in to any building for which you do not have access. As the Ombudsman's office we have a requirement to ensure the confidentiality of all complaints through this office and therefore anyone who is not an Ombudsman employee is required to sign in and be escorted. This includes but is not limited to DND employees and military members as well as staff's personal visitors (spouses, children, etc.). Several policies across the government support this practice including the Policy on Government Security as well as the National Defence Security Orders and Directives. The Urbandale security policies developed and implemented by Public Service Procurement Canada (PSPC) security, who are responsible for the security of the Urbandale building, also require a sign in log be kept of all non-Urbandale employee visits to this building.

There are several reasons for which this policy is being used:

As an office, we are responsible for the safety of all visitors on our floors. Should there be an emergency, we are able to ensure the safe evacuation of our visitors through our emergency volunteer organization and can confirm their safety using our roll call procedures.

Having visitors sign in also allows us the protection of our assets. Should assets/equipment/documents or files go missing during or after working hours, the

sign in log allows us to know who was in the office and when so that if required these individuals could be questioned during an investigation.

The protection of staff is also of utmost importance. Should there be a breach of security involving visitors to the office the visitor log allows us to have the names of individuals and the times in which the individuals were signed in/out. It also allows staff to distinguish who is an employee and who is a visitor.

Organizers of meetings or group visits must advise the commissionaires in advance by completing the form available on the shared O:\ drive. A copy of the form mentioned above must be given to the commissionaire post.

The form can be found in the following location:
O:\Administration\Administration Forms\Security – See also Annex B

For safety reasons access afterhours for non-employees including family members is not encouraged. Those employees that wish to request access must have explicit written permission from their Manager and the USS must be informed so that there is a clear record of the visit.

3.3.5 Piggy Backing

It is the responsibility of all staff to ensure that non authorized individuals do not enter the main building entrance after hours. If you are entering the building before or after hours and an unknown individual attempts to enter behind you, you are to request that they swipe into the building. Regardless of whether or not they are wearing Departmental ID Cards they may not have their department's authorization to enter the building before or after hours.

It is the responsibility of all staff to ensure that anyone getting off the elevator on the 13th floor is an Ombudsman employee. No access is permitted for non-Ombudsman employees to the 13th floor unless accompanied.

3.4 Security Screening

3.4.1 Reliability Status and Security Clearances

The security screening level requirement is to be indicated on work descriptions, staffing and contract documents. Before an offer of employment, contract or assignment is made, the individual must obtain a DND issued enhanced reliability check and must then be able to obtain and maintain the required clearance level for the position. If an individual is not able to maintain it, a termination or other consequences may take effect.

An enhanced reliability check is considered good hiring practice; it is used to determine the reliability of an individual before they commence work and includes a criminal records check as well as a credit check.

Information cannot be collected for security clearance purposes without the written consent of the individual. Persons who do not consent to processing of the necessary checks cannot be considered for employment, contract or assignment.

For reliability status, a personal and employment data check is required. The hiring manager must conduct a reference check and a verification of education, addresses, employment and identity, and must then consult the Unit Security Supervisor to complete the appropriate documents confirming this has been completed.

Please see the Treasury Board Standard on Security Screening for guidance on how to complete these checks.
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115

3.4.2 Renewals

The Unit Security Supervisor will initiate clearance renewals and ask individuals for updated information to process the appropriate checks. A Reliability Status, Level l and Level ll clearances must be renewed every ten years. A Level III clearance must be renewed every five years.

3.4.3 Denial

Please see Appendix D, section 18 of the Treasury Board Standard on Security Screening for information concerning the denial, revocation and suspension of clearances.
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115

3.4.4 Briefings

A security clearance briefing is mandatory for every person working in the office. The Unit Security Supervisor provides briefings when the individual begins working at the Office.

3.4.5 Transfers / Reinstatements

A military individual who begins working for our office that has had no break in service of 24 hours or more may have their current clearance transferred / reinstated to civilian status (using their PRI to replace their military service number)

without undertaking the entire clearance process again. However this process still requires the completion of the security forms 330-23 and 330-60 if required. The purpose of completing these forms is to update the employment, residential, marital status and any other information that may have changed since they last completed the forms.

3.5 Keys and Combinations

Employees are responsible for the safeguarding of information and equipment in their possession. Keys to offices are not to be copied and are the responsibility of the individual to whom they have been assigned. Loss or theft of keys should be reported to the Unit Security Supervisor immediately. Combination locks and combinations are also the responsibility of the individuals to whom they have been issued. Combinations should not be shared, revealed or kept in locations where they can be found and used by unauthorized personnel. Any incident must be reported promptly to Unit Security Supervisor.

The Unit Security Supervisor issues padlocks and office keys. Combinations are to be set by the user and a copy of the combination given to the manager and the Unit Security Supervisor. Managers must ensure combinations are changed when users depart, no longer need access or when combinations have been compromised. Individuals who are issued cabinets with integral combination locks (that can hold information up to Secret) must ensure the combinations are changed once every 6 months and a record of the change is kept on a change card kept inside the cabinet and a copy given to the Unit Security Supervisor. For the sake of audit purposes, the Unit Security Supervisor can ask to see the record of combination change at any time. The Unit Security Supervisor maintains a register of keys and combinations.

Managers should also keep a list of combinations issued to their staff. They must ensure that the list is kept in a sealed envelope under the control of one individual, stored in a locked security container suitable for storing information for which the key or combination provides access and marked with the highest sensitivity contained.

Please visit the Treasury Board's Operational Security Standard on Physical Security: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329

The required forms and envelopes are available from the Unit Security Supervisor.

3.6 Storage

3.6.1 Desk and Work Area

Employees have the responsibility for maintaining the security of their own work area. Desk and work areas are to be kept clean and secure as much as possible during working hours and are to be secured when leaving the Office at night (including recycling and garbage bins as well as in-boxes and mail boxes).

3.6.2 "Lock-up"

According to the RCMP Security Equipment Guide, the definition of "lock up" is the requirement for storage of Protected A and Protected B information in an operations zone. Information is considered "locked up" during business hours if it is only accessible to those with a need to know.

During working hours, if you will be away from your desk for only short periods of time it may be sufficient to simply move information from casual observation (i.e. flip the pages you are working on, put them in an unmarked folder, put them in a drawer, or close an office door). **It is up to the individual working on the documents to manage the security of their documents.**

Please note: It is recommended that you lock your computer screen when you get up from your desk. Do not wait for the time out to take effect. This will prevent unauthorized viewing of documents or access to documents on your computer screen.

If you will be away from your desk for extended periods of time you should afford the level of security to the documents that you would if you were leaving for the day, or for longer periods of time such as vacation etc.

More information on lockup can be obtained by visiting the following link:
http://www.rcmp-grc.gc.ca/tsb-genet/seg/html/page_0014_e.htm.

Storage requirements outside of work hours or when not being used:

Classification/Designation	Storage Requirements
Protected A	Stored in locked cabinets.
Protected B	Stored in locked cabinets with dial lock combination or approved padlock.
Protected C	Consult with the Unit Security Supervisor for requirements.
Confidential	Stored in locked cabinets with dial lock combination. This does not include your office filing cabinet. Please see the USS for your storage requirements. We have one filing cabinet approved for storage of this level of material.
Secret	Stored in locked cabinets with dial lock combination. This does not include your office filing cabinet. Please see the USS for your storage requirements. We have one filing cabinet approved for storage of this level of material.
Top Secret	Consult with the Unit Security Supervisor for requirements.

3.6.3 Open Shelf Storage

Open-shelf storage of protected or classified information or bulk storage of other valuable assets (e.g., computers, expensive or critical equipment) must be done in approved secure rooms. These rooms are built in accordance with the level of confidentiality or importance of the assets to be kept within them. Access is strictly limited to authorized employees.

3.6.4 Occupant away signs

Individuals should use the Occupant Away sign provided by Unit Security Supervisor in order to prevent sensitive information from being left on their desk when the occupant is away. **No information is to be left in a cubicle without the receiver's presence.**

3.6.5 Personal Property

Employees are responsible for the protection of their personal property. Purses, wallets and money should be kept in personal custody at all times, or locked in a secure cabinet or area. When leaving your work station please ensure that any valuables are out of sight to prevent any incidents. The office cannot be held responsible for loss of personal items as long as the above is being applied.

3.7 Mailing

All mail containing classified or protected information must be packaged and transmitted in accordance with the chart below and in accordance with section 8.4 of the Treasury Board's Security Organization and Administration Standard.
http://tbs-sct.gc.ca/pol/doc-eng.aspx?id=12333&section=text

Marking	PROTECTED A PROTECTED B	CONFIDENTIAL & SECRET	TOP SECRET & PROTECTED C
Packaging	1 gum-sealed envelope or single sealed wrap/box. No security marking. Within Office: economy envelope or labeled folder is acceptable.	Except for delivery outside Canada (see below): 1 gum-sealed envelope or single sealed wrap/box. No security marking. Within Office: economy envelope or labeled folder is acceptable.	2 gum-sealed envelopes. Double-sealed wrapping of bulky or heavy packages. Address on both. Security marking and "To be opened only by" on inner envelope or wrap. Record must be kept of documents sent.
Delivery within Office	Internal mail	Internal mail in a sealed envelope	Hand delivered in a sealed envelope
Delivery within the NCR	1st class mail or messengers with approved briefcase	Messengers cleared to Secret; must use a locked security briefcase for deliveries to, and from Office facilities. First class mail may be used in a double envelope with security marking and To be opened only by on inner envelope or wrap. Record must be kept of documents sent.	Messengers with a Top Secret clearance; must use a locked security briefcase for deliveries to, and from Office facilities.

Marking	PROTECTED A PROTECTED B	CONFIDENTIAL & SECRET	TOP SECRET & PROTECTED C
To other Canadian cities	1st class mail	*Confidential* - First class mail with recorded transit and delivery or by reliable commercial courier *Secret* – reliable commercial courier with recorded transit and delivery	Registered Mail
Delivery outside Canada	First class mail or, if urgent, reliable commercial courier.	Packaging and delivery same as for TOP SECRET.	Diplomatic Security Mail Service. Address outer envelope to Distribution Services Division (SBG), DFAIT. Exact destination address and security marking must appear only on the inner envelope. Place a "Transmittal Note and Receipt" form (GC 44) in inner envelope. Seal inner envelope (or wrap) with approved security tape.

3.8 Destruction

All protected and classified information must be destroyed by a machine shredder approved to the level of the sensitivity of the information. For more information, contact the Unit Security Supervisor.

The office has approved shredders (in accordance with the Security Equipment Guide and the Government Security Policy) for small volumes of shredding up to and including, Secret documents. Disposal of large quantities of sensitive material must be arranged by contacting the Unit Security Supervisor and done in accordance with appropriate Government of Canada guidelines and internal IM SOPs.

Use the following links for information to these policies:

- RCMP Security Equipment Guide, Section 2
  http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0068_e.htm

- Policy on Information Management
  http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/mgih-grdg_e.asp

- Internal Information Management SOP on Managing Disposition
  O:\RKI\SOPs\Managing Disposition

DVDs and CDs containing sensitive information must be disposed of in an approved manner. Hard drives and other electronic equipment, including fax memory cards, containing sensitive information must be disposed of by contacting the Unit Security Supervisor. The Unit Security Supervisor will ensure these items are destroyed at an approved shredding facility.

Use the following policy for more information:

- RCMP Security Equipment Guide, Section 3
  http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0069_e.htm

For more information on the destruction of information, please see Legal Services or your Unit Security Supervisor.

3.9 Telephones

Telephone communications are especially at risk of interception by unauthorized individuals. To reduce the risk of interception and unauthorized disclosure, the following procedure should be followed:

1. Cellular or other wireless telephones, including cellular telephones integrated into Blackberry devices, must not be used to discuss any type of sensitive information. These telephones transmit over radio frequencies that can easily be intercepted.

2. In cases where a secure telephone is not required and where calls are made to and from locations outside of the telephone exchange system, care must be exercised to reduce the risk of interception of sensitive conversations on LAN telephones. Avoid discussing sensitive information or limit the amount of such information to be discussed and the level of detail.

Note: LAN (local area network) telephones are regular phone lines connected via telephone jack. They are not wireless phones i.e. cell phones, BlackBerry, satellite phones, etc.

3.10 Fax

Fax communications are routed by telephone and are subject to the same risk of interception as described in the previous section. In addition, unauthorized individuals could see sensitive information if a wrong number was to be dialed. The amount of information that can be faxed is normally greater and more factual than could be discussed on the telephone. The information can also be easily photocopied. It is therefore required that:

- Protected B and Classified information is not to be faxed; and
- Care should be exercised when faxing less sensitive information (i.e. Unclassified or Protected A) to ensure that the intended party receives the information.

3.11 Laptops and Office Computers

Only approved office laptops and computers that are equipped with appropriate security software can be used for processing sensitive information. In other words, this means you are not authorized to use your home computers to process information.

Top Secret, Secret, Confidential and Protected C information must **NOT** be processed on any computer within the office. To process Confidential and Secret information electronically, please see the USS.

When working from laptops; in order to process Protected B information, users must use either a Protected A laptop or a Protected B and no other means (i.e. home computer). The following must be respected:

- Protected B information cannot be stored on a Protected A machine. You must use an office issued USB stick to store the information once you are finished working on it;

- You must use your PKI card in conjunction with the Protected B laptop in order to access the system;

- No information whatsoever should be saved on the hard drive of the laptop;

- No electronic transmission is permitted using the Protected B laptop. If transmission is required, the information will need to be transferred to a USB stick then the use of a Protected A laptop will be required to send an encrypted e-mail using the PKI (Entrust) system;

- Keep any written record of the password separate from the PKI card. The password should be memorized. Do not leave the laptop unattended once the card and the password has been entered;

- Remove the card from the laptop when it not being used. Store the card in an approved briefcase or filing cabinet. Store the laptop in a separate locked location which provides reasonable protection from unauthorized access;

- Secure any USB stick containing sensitive information, and any document that is printed from the laptop, in an approved briefcase or filing cabinet;

- You must keep the laptop in your possession during transport. Where feasible, use an approved briefcase to transport the PKI card and keep the briefcase under personal custody or in a secure area. On a plane, users should check the laptop as luggage and keep the briefcase with them as a carry-on;

- Carry USB sticks separate from the computer;

- At the Office, store the laptop in a locked security container;

- Out of the office, keep the laptop with you or store it securely (e.g., out of sight in the trunk of the car, in a safe location in the home or hidden way from view in a hotel room); and

- Report immediately any suspected or actual compromise to the Unit Security Supervisor (e.g., unauthorized access, loss, theft, tampering) of the PKI card or the laptop. Upon return of a laptop, the Unit Security Supervisor will ensure that the machine is wiped clean before it is issued to future users.

3.12 Public Key Infrastructure (PKI) Cards / Entrust

The DND Public Key Infrastructure program is a system designed to process and transmit Protected B information on a Protected A machine. All indeterminate employees of the Office must possess a PKI card.

The user subscriber agreement that you signed when you were issued your card for the security regulations stipulates the following (taken directly from the agreement):

a) You require an enhanced reliability to be a user;
b) Your user ID, password, and authentication tools or other IT security devices are for your personal use only, and shall not be given to or shared with any other personnel and shall be secured at all times;
c) Your digital signature is as legally binding as your hand-written signature;

d) You are only allowed to access and/or copy data that is specifically required and authorized for your use;
e) You are not to provide unauthorized users access to the above mentioned resources;
f) You shall use your privileges for access to the resources for authorized use only;
g) All of the designated domain information and IT material that you may have been given access to shall be secured in accordance with Government Security Policy and the National Defence Security Policy/Instructions;
h) You are responsible for providing reasonable care for the resources while they are in your custody;
i) You shall observe all software license restrictions with respect to DND PKI resources, which you are granted user access;
j) It would be a contravention of these rules should you, without lawful authority:
    - Communicate any information that you have been granted access to;
    - Use any such information or DND PKI resources for other than authorized purposes;
    - Destroy or alter data;
    - Render meaningless, useless or ineffective; and/or
    - Obstruct, interrupt or interfere with the lawful use of data.
k) The DND PKI cannot be held responsible or liable for any loss, damage, or disruption or personal activities or personal data, which may result from use, or loss of use of the above noted resources;
l) You take full responsibility for your actions and understand that any violation of the spirit or intent of the DND PKI access rules and regulations can lead to loss of privilege or further actions; and
m) You understand your role and accompanying responsibilities and have been briefed in accordance with DND PKI procedures.

For more information on the use of PKI cards please see your Unit Security Supervisor.

3.13 Desktop Computers

3.13.1 Time out

The Protected A and Protected B systems require time out capability. As per DND / info secure policy, the Protected A system time out is decided for us and cannot be changed. The Protected B timeout has been set equivalent to the Protected A system. However it is recommended that you do not wait for the time out to take effect. If you get up and walk away from your desk you should be locking your screen to prevent unauthorized viewing or access to your computer.

3.13.2 Passwords

It is everyone's responsibility to ensure passwords are properly safeguarded and managed. Do not share passwords.

The use of passwords on Word, Excel and other documents is a way to provide controls on shared sensitive documents. Passwords must be stored with the respective manager for reference purposes and are not to be circulated with the document. This is especially important when an employee leaves the office.

To password protect a document, please see Annex C.

3.13.3 Network Account Briefings

All users must take the network account briefing when they are first issued their account. The Unit Security Supervisor completes the briefings. Please see the following policies regarding this requirement:

- Treasury Board Policy on Acceptable Network and Devise Use: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27122

- DAOD 6002-2, Acceptable Use of the Internet, Defence Intranet, Computers and Other Information Systems: http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6002-2.page

3.13.4 Email

It is important to ensure that when sending emails they are being sent to the correct individuals, one way to ensure this is to add frequently used contacts to your address book. Another is to scan your to list and ensure you have the correct addressees.

The office uses a standardized signature block; please see Annex J for more information.

As part of the standardized signature-block the office has adopted an email disclaimer. This disclaimer along with your signature block should be used when sending new email and when replying to and forwarding email.

The email disclaimer should also be used on your BlackBerry signatures.

3.14 USB Sticks / CD / DVD

As per DND policy, personal USB sticks, CDs and DVDs (i.e. those not issued by the Office) are not to be used on any DND computer.

Please note that USB sticks, CDs or DVDs that contain any Protected (A or B) information are not to be used on home computers including the Rogers Stand Alone computers located in this office. This is due to the lack of protection that is afforded to the information on a home computer. Home computers are susceptible to viruses that could destroy or compromise sensitive information.

USB sticks are not to be left in computers; they are to be locked up when not in use.

If a USB stick contains only unclassified material and you use your Office issued USB stick on stand-alone computers, you must scan the device for viruses each time before using it on your Office computer. See Annex D on how to scan your USB stick.

The same directive applies to all other electronic files that are brought in via CDs or DVDs. They must be scanned before being used on the DND system to ensure no viruses are being introduced and they must be password protected to protect the information contained on them.

Personal phones and tablets are NOT to be plugged into a DND computer.

3.15 Sensitive Information Outside the Office

Employees who need to take or work on, sensitive information outside of the office must safeguard the information at all times from unauthorized disclosure, viewing or overhearing. They must avoid conversations of a sensitive nature in areas where unauthorized persons could overhear them and do so only with approval of their managers.

The following safeguards apply to Protected A and Protected B sensitive information:

Outside of the Office

Individuals who bring such information to meetings outside of the Office should:

- Use a locked approved briefcase and keep the briefcase with them when they are in transit;

- During extended breaks (e.g., lunch), leave the briefcase or the information in a location approved for the storage of such information, or bring the briefcase with them and keep it under their control;

- For overnight stays, leave the briefcase or the information in an approved secure location at the meeting area or at a Canadian diplomatic mission abroad. If secure storage is not possible, keep the information in the locked briefcase in the hotel room or other accommodation and hide the briefcase from view; and

- Not process, store, transmit or discuss such information on systems (e.g., computers, telephones, fax equipment) that are not approved for that level of information.

At Home

Employees who intend to use an office issued computer to work at home:

- Should ensure that their supervisor is aware that they are doing so. They must use a locked approved briefcase to transport the information and must protect the information at all times from unauthorized disclosure. Individuals who regularly bring such information at home must use an approved security container to store the information.

- Do not share your briefcase lock combinations with anyone.

3.16 Security Infractions

Security infractions are acts that contravene the requirements of the Office security policy and its associated documentation, and which could result in compromised security.

They include the failure to store sensitive information and lock filing cabinets outside of work hours, protect access cards and passwords, and transmit and dispose of sensitive information in accordance with approved security procedures.

Where security checks are conducted, infraction notices are left if storage containers are found unlocked, if sensitive material is not stored properly or if computers are not properly logged off at the end of the day. Any such material will be secured or removed and kept by the Unit Security Supervisor until the owner claims it. A copy of the infraction notice will be given to the appropriate managers and an additional copy will be kept in the individuals security file. In cases where the same individual receives several infraction notices, the Unit Security Supervisor will discuss remedial action with the appropriate manager.

See Annex I for more information on Security Checks

3.17 Business Continuity

A Business Continuity Planning (BCP) Program is a risk management strategy to mitigate the potential impact that service disruptions may have on corporate business activities. This risk mitigation strategy approach is based on an assumption that business disruptions will happen. As a result, plans need to be put in place, that can be tested and that are maintained and updated yearly, in order to ensure that the Office of the Ombudsman can continue to meet the requirement to its constituents.

An emergency is an abnormal situation that requires prompt action in order to limit injury to personnel and compromise to assets. It can be caused by accidents or events such as fire, bomb, chemical or biological or nuclear incidents; cyber-attacks; power failures and natural disasters (e.g., earthquakes, floods).

Management must ensure that emergency and business continuity plans, including IT contingency plans, and procedures are developed, tested and kept up-to-date in order to effectively respond to, and recover from, emergencies, and continue the delivery of essential and critical services and functions until normal operations are resumed. Assets that support critical services and functions must be identified. Measures must be taken to ensure their availability in the event of an emergency. Back-up capabilities and off-site storage are elements of this capability.

The Office of the Ombudsman business continuity plan can be found in the following location – O:\Administration\Security\Business Continuity Plan

Please note that all staff is responsible for reading the BCP. It is for their own benefit and safety that they must read and understand this plan. If there are any questions about the BCP and its content please contact the BCP coordinator, in this case the Director of Corporate Services or the Unit Security Supervisor.

3.18 Removal of Property

Personnel wishing to bring laptops or other valuable equipment outside of Office facilities must obtain their supervisor's authorization in writing and must obtain a form from the Unit Security Supervisor. They may be asked by the building security personnel to show such authorization. They should keep the authorization with them each time they enter a new facility as they may be required to show authorization and proof of DND ownership at any government building.

3.19 Physical Security

3.19.1 Panic Buttons

At reception and in the interview room there are two panic buttons. When they are pressed they will send a strobe light to the entire 12th & 13th floor but they will also alert the commissionaires in the lobby who will:

1) Call 911 for assistance;
2) Notify the Unit Security Supervisor or alternates of the situation; and
3) Notify the building operators.

Please ensure that you do not press the buttons unless you require them in an emergency.

If one is pressed accidentally please ensure you call the Commissionaires immediately at 949-7243 to advise them of the false alarm and then call the Unit Security Supervisor (or alternates) to report the accident.

Once the button is pressed in a real emergency, please ensure you attempt to remove yourself from the situation. As you are leaving the room please take the envelopes located by the exits, which contain emergency contact information that you can use to assist yourself in the emergency. If the incident occurs in the reception area, the individual is to enter the operations zone through the second reception door. There is an envelope located by the exit that contains contact names and numbers. Find the closest available phone and call the Unit Security Supervisor. The same process applies if the situation occurs in the interview room. The individual should exit through the door that leads into the operations zone and again should take the emergency envelope with the required information.

If you are unable to safely leave the area you are in without providing the threatening individual access to the operations zone please remain calm and understand that by pressing the panic button the appropriate individuals will respond to the alert.

It is important to note that if you hear the emergency siren that you do not enter these areas. Be assured that the authorities have been notified and that you are not required to attend to the situation.

PLEASE NOTE AN ANNUAL TEST OF THE SYSTEM WILL BE PERFORMED. YOU WILL BE NOTIFIED PRIOR TO THE TEST TAKING PLACE.

3.19.2 Security Alert Level Program

Based on past security incidents, it was decided that a security level alert program for the office needed to be implemented. This program will allow the Unit Security Supervisor to quickly provide information to staff on possible threats to the Office and to handle those threats from a security perspective.

As part of the Government Security Policy, it is management's responsibility to ensure a safe working environment for all staff. This program is appropriate for dealing with the types of threats that are received while allowing the office to continue daily operations by balancing the need for security with the need for efficiency and a certain degree of openness towards constituents, the people the office deals with as part of its work, and the general public. Each level is meant to reflect more stringent security measures which may be required at different times, to respond to elevated threat levels, either generally or specific to the Office.

The Privy Council Office can initiate changes to the level of security for the government as a whole, and the Office of the Ombudsman's Unit Security Supervisor, in consultation with senior management, can initiate changes specific to this Office. Staff members are expected to familiarize themselves with these measures, and are responsible for complying with and assisting to implement the relevant measures.

The first section of this document is the procedure for reporting potential or actual security incidents, which in turn can lead to the elevation of the Office's security level.

Reporting Security Incidents:

Security incidents are to be reported in the following manner:

1) They are to be reported immediately to the Unit Security Supervisor (or alternate should the Unit Security Supervisor be away) either by phone or by direct contact.

2) Advise your supervisor of the situation at hand and that you have notified security.

3) You should remain available to provide information to the Security Committee and / or to Security Authorities where necessary

4) Be sure to remain calm and write down / document as much information as possible including:
    - Individual's name / phone number / address;

- Time and date of call;
- Physical location of the individual making threats; and
- Anything the individual says – including the individuals against whom the threats are being made.

**Security Handbook sections – 3.20.2 to 3.20.8 provides detail on dealing with threatening situations*

***PLEASE NOTE: For Bomb Threats please see Annex F of this document for procedures*

The Unit Security Supervisor will:

- Notify / gather the required key parties for an emergency meeting – these individuals include members of the senior management committee, and the individual who reported the incident;
- Implement an increased Security Alert Level where required; and
- Notify staff of level increases and provide information and pictures as required regarding the incident at hand.

The Committee will:

- Determine the threat level and assess the risk to staff, and
- Decide what Security Alert Level to put in place.

Security Level Alerts

The default condition is Green, and staff will be advised by phone or direct contact (or by email where no imminent threat exists) when more stringent measures are in place, as well as the duration of those measures (if known).

Green – Business as Usual

- Current Security Standards already implemented include:
  - Commissionaires verifying passes at the entrance to the lobby;
  - Security cameras in building lobby as well as on the 12th floor (reception and interview room) and 13th floor (near large boardroom);
  - Panic buttons at reception and in the interview room - staff should be familiar with their location, and should use them if they feel their physical safety is threatened. Staff should be familiar with the sound generated when the panic button has been activated, and what to do in that case;
  - Intercom at reception;
  - Interview room controlled by a 2-door system and a swipe card system; and

    - Swipe access to all doors on both floors and on the 13th floor through the stairwells and elevators.
- Standard security procedures – for both floors.
- All staff should have their building passes with them at all times while on the 12th and 13th floors, and they should be visible while in the lobby or on another floor that we do not occupy.
    - As per The Operational Security Standard – Readiness Levels for Government Facilities.
      http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12331
      The Government of Canada is currently at Level Readiness Level 2 but this is subject to change.
- Visitors must report to Commissionaires in the main lobby who notify the contact listed on the meeting form. See Annex B
    - Visitors should be announced to Commissionaires prior to meetings taking place using the Commissionaire's meeting form:
      O:\Administration\Administration Forms\Security
- **No** piggy-backing at any time from any entrance into the facility or entrances / exits on the 12th and 13th floors.
- Visitors arrive in the lobby, sign in and obtain a visitor pass and then they are escorted by the employee they are visiting into the office space.
- Swipe access to all operation zone doors.

12th floor – Unsecured Floor

- **No** piggy-backing.
    - This is for the safety of everyone in the office.
- Optional security item includes the reception intercom for communicating to visitors.
- Interview room is to be used for walk-in complainants – individuals are not to enter operational work space. They must sign in but are not required to wear visitor passes. Staff is to let walk-ins into the interview room through the reception area.

13th floor – Secure Floor

- Secure swipe access through elevators and stairwells.
- Visitors on the 13th floor are to go directly to the elevators. They are not to be left unattended there.

Yellow – Warning

Each incident will be evaluated separately, for appropriate security measures.

Includes all Green Level precautions, and also includes the following:

- Staff are asked to be vigilant of all individuals and report any sightings of unwanted individuals to the Unit Security Supervisor and to Legal Services.
- Distribution of pictures and any available information to all staff concerning the situation at hand.

12th Floor – Unsecured Floor / 13th Floor – Secure Floor

- Reception Lock Down
    - Commissionaires to escort all individuals up to the 12th / 13th floor including those with DND ID.
    - Visitors are not to be left unattended at any time.
    - Mail / Courier are picked up in the 12th floor lobby by the mail clerk or another designated individual.
    - Instructions will be given for dealing with specific threatening individuals on the telephone or for dealing with threatening individuals who may attempt to gain entry to the Office.
- Staff may be asked to avoid using reception or other entrances to avoid piggy backing into the reception area as directed by the Unit Security Supervisor.

Red – Full Security Protocol

Each incident will be evaluated separately for appropriate security measures.

- Includes as possible security measures:
    - The possibility of building evacuation or shut down (full lock down);
    - No visitors allowed into the building or on the 12th and 13th floors;
    - The possible placement of security guards on the 12th and 13th floors;
    - Possible activation of the Business Continuity Plan depending on the nature of the incident; and
    - The involvement of security authorities, i.e. Military Police (MPs), Ottawa Police, or RCMP.

Please note that in the case of the Red Level, as there are a wide range of possible security measures. If the Red Level is deemed appropriate to address a security incident, exact instructions regarding those measures that will be implemented will be provided to staff at that time.

3.20 Emergency Procedures

3.20.1 Emergency Procedures

Please visit O:\Health and Safety\Emergency Procedures for the Urbandale Emergency procedures.

Please note that in addition to the Fire Emergency Procedures the office has adopted an additional Roll Call procedure that is over and above the Building Fire Emergency Procedures. These procedures can be found in Annex H.

Please note that personal heaters, coffee makers, and hot plates of any kind are not authorized in your cubicle or office.

Personal fans may be authorized on a case-by-case basis.

Please consult the Office Small Appliance Policy for more information on what is approved for use within the office. This policy can be found in the following location: O:\Health and Safety\Internal Programs & Policies\Small Appliance Policy\Small Appliance Policy (Eng)

Please see your Unit Security Supervisor for authorization.

3.20.2 Threats

The motivation for individuals to introduce radioactive, explosives, biological and chemical agents into a Government complex varies considerably. Examples may include: a terrorist act; wanting to inflict injury to senior officials; wanting to make a statement by adversely affecting government operations; the desire to cause harm to employees; or a challenge of finding ways to circumvent control measures.

Threats are a fact of life in today's environment. They vary in scale from global to localized threats. They may be directed at a specific building, department or at specific individuals. Whether real or perceived, threats pose serious safety concerns and have the potential to disrupt normal operations.

Our office receives threats from time to time from angry callers. In the event that threats against staff members are received, the following procedures should be adhered to:

1) Caller receiving the threat against another employee should be careful to write down the name of the person giving the threat, as well as take down the phone number from which the individual called, they should also confirm the location of the individual calling and write down as many details from the conversation as possible.

2) The employee should then notify; their manager, the Unit Security Supervisor and Legal services immediately providing all of the details above.

3) The lead in these situations will then be undertaken by the Unit Security Supervisor in conjunction with Legal Services, the Director of Corporate Services, the Director General of Operations and the Ombudsman.

4) All staff will be notified of the potential threat to safety with specific instructions where there is thought to be a danger to staff.

5) The Unit Security Supervisor will take care of escorting police and other security professionals where required and will be the primary liaison with building security.

3.20.3 Reception Lock Down

When threats are received, the USS can decide to lock down the reception area. This area must be part of the lockdown even though it is no longer in use. It is still an entrance point to the office.

3.20.4 Walk In Complaints

The office does receive walk in complainants. Usually these are handled by the Intake Officers. All walk in complaints are to be dealt with in the Interview Room and must be done by 2 individuals. Employees are not to take walk in complaints alone. In cases where the walk in complainant becomes angry, threatening or otherwise a danger to the employees or this office, they are to be asked to leave and the incident reported to the USS immediately. Do not follow these individuals out of the building. Once you advise the USS the building Commissionaires will be notified to ensure the individual leaves the premises. If the individual will not leave you can chose to excuse yourself from the room and call the USS for assistance (when both doors are closed the individual inside cannot leave the room without a pass) or if you feel you are in danger you can use the panic buttons to alert authorities.

3.20.5 Suspicious Mail and Packages

The main threats related to mail and parcels are related to exposure to radiation, explosives, biological and chemical agents.

A suspicious package is just that — a package or envelope found or received which raises the suspicion of the receiver or person handling it. It can be via normal mail, special mail, by courier or delivered in person. It may or may not be preceded by letter or telephone threats or warnings. Each type of suspicious package poses separate threats and they should not all be dealt with the same way.

When discussing suspicious mail and packages, the paramount consideration is the health, safety and security of occupants of the building. The Canada Labour Code and other Acts and Regulations stipulate the obligations of employers, and others responsible for building occupants, to plan for emergencies and to practice "due diligence" to reduce hazards and risks in the workplace. Thus, all possible actions and precautions must be taken. In case of doubt, the safest course is to err on the side of caution.

3.20.6 Suspicious Objects/Substances

Dangerous objects/substances could be a suspected chemical spill, toxic fumes, and a biological or radiological substance.

- **DO NOT TOUCH** suspicious objects;
- Inform your manager and Unit Security Supervisor; and then
- Inform the Fire Department and the building Emergency Organization; and
- Maintain the integrity of the area;
    - Keep personnel away from the object/substance, and
    - If possible isolate or cover the object/substance.

For more information on dealing with suspicious objects/substances, please see Annex F.

3.20.7 Bomb Threats

An individual can receive bomb threats in person, by telephone, or in written form including by email, social media (Facebook, Twitter) and Live Chat.

Telephone Bomb Threats

- Listen carefully, be courteous and permit the caller to say as much as possible without interruption;
- If possible, ask and note: What time will the bomb explode? Where is it? What does it look like? Where are you calling from? Why did you place the bomb? What is your name?;
- Record date, time, and duration of call and exact wording of the threat;
- Identify individual characteristics: sex, accent, voice (loud, soft), speech (fast, slow), diction, manner;
- If your telephone has the CALL DISPLAY feature, note the information;
- Inform your manager and/or the Unit Security Supervisor who will then;
- Inform the Police and the building Emergency Organization of the threat; and
- Complete the Threat Telephone Checklist. See Annex E

In Person Bomb Threats

- Do not antagonize the individual(s);

- Follow instructions and be alert;
- Avoid being hostile;
- Don't speak unless spoken to;
- Maintain the integrity of the area if you are not in danger;
- Inform your manager and/or the Unit Security Supervisor who will then inform the police of the threat.

Suspected Bomb

- **DO NOT TOUCH**;
- Inform your manager and Unit Security Supervisor and then;
- Inform the Police (DO NOT USE RADIO or CELL PHONE);
- Maintain the integrity of the area; and
- Keep personnel away from the object.

3.20.8 Threatening/Crank Calls and Letters

Phone Calls

- Listen carefully, be courteous and permit the caller to say as much as possible without interruption;
- Record date, time, and duration of call and exact wording of the threat;
- Identify individual characteristics: sex, accent, voice (loud, soft), speech (fast, slow), diction, manner;
- If your telephone has the CALL DISPLAY feature, note the information;
- Inform your manager and the Unit Security Supervisor who will then;
- Inform the Police of the threat.

Letters

- Avoid excessive handling;
- Preserve all materials as evidence;
- Inform your manager and the Unit Security Supervisor who will then;
- Inform the Police.

Email

- Do Not Delete;
- Inform your manager and the Unit Security Supervisor who will then;
- Inform the Police.

Voice Mail

- Do Not Delete;
- Inform your manager and the Unit Security Supervisor who will then;
- Inform the Police.

Annex A – Summary Table – Classified / Protected Information

Summary Table:

LEVEL/MARKING	DEGREE OF INJURY TO THE NATIONAL INTEREST	DEGREE OF INJURY TO OTHER INTERESTS
TOP SECRET	Exceptionally Grave	
SECRET	Grave	
CONFIDENTIAL	Limited	
PROTECTED C		Exceptionally Grave
PROTCTED B		Grave
PROTÉCTED A		Limited

Annex B – Meeting Form

Ombudsman

National Defence and Canadian Forces | Défense nationale et Forces canadiennes

MEETING / RÉUNION

Date / Date:

Time / Heure:

Floor / Étage: th Floor / étage

Contact Person / Personne responsable:

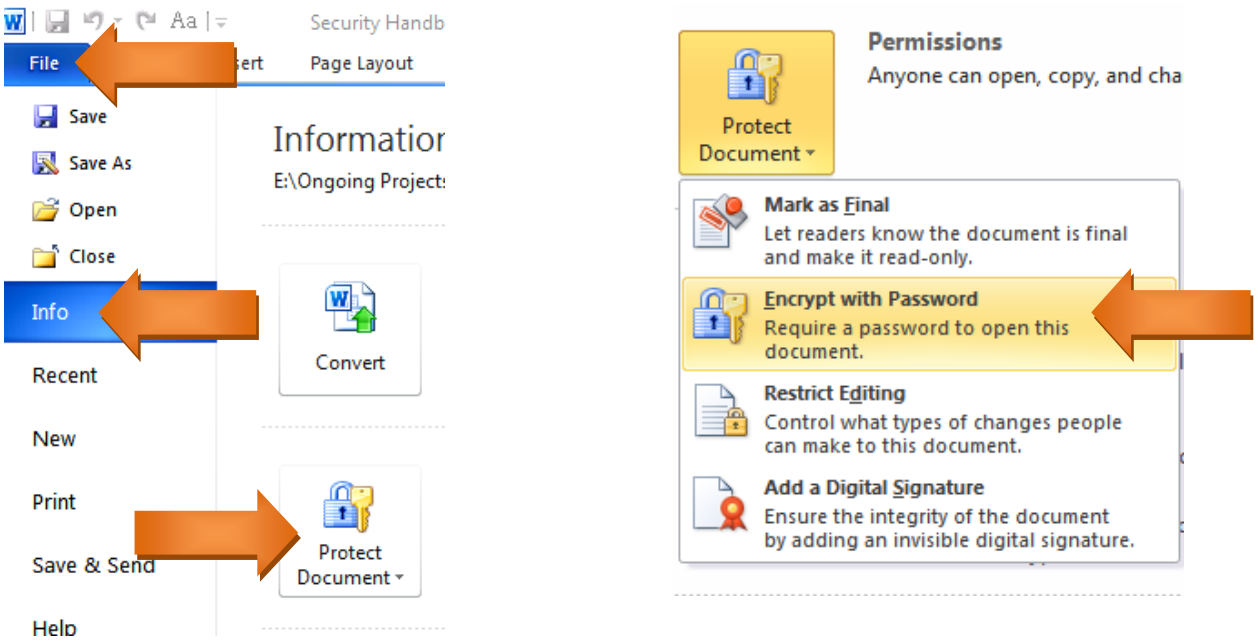
Telephone Number / Numéro de téléphone:

Attendees / Participants	Department or Agency / Ministère ou organisme

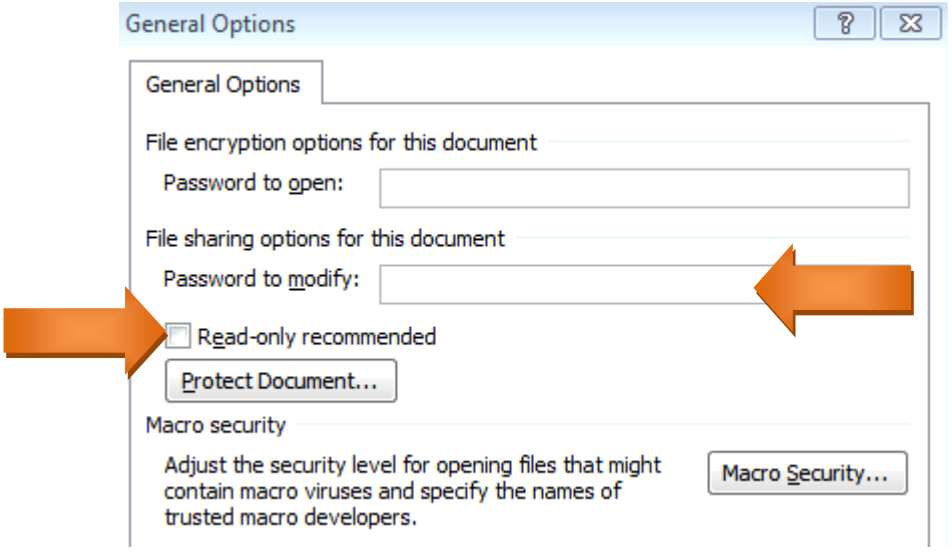
Annex C – How to Password Protect Documents

In Microsoft Word 2010

Go to File / Info / Protect Document / Select the Encrypt with Password option. You can use a password to open, to modify and/ or you can chose "read only recommended", you can use all three together or in any combination that you want.



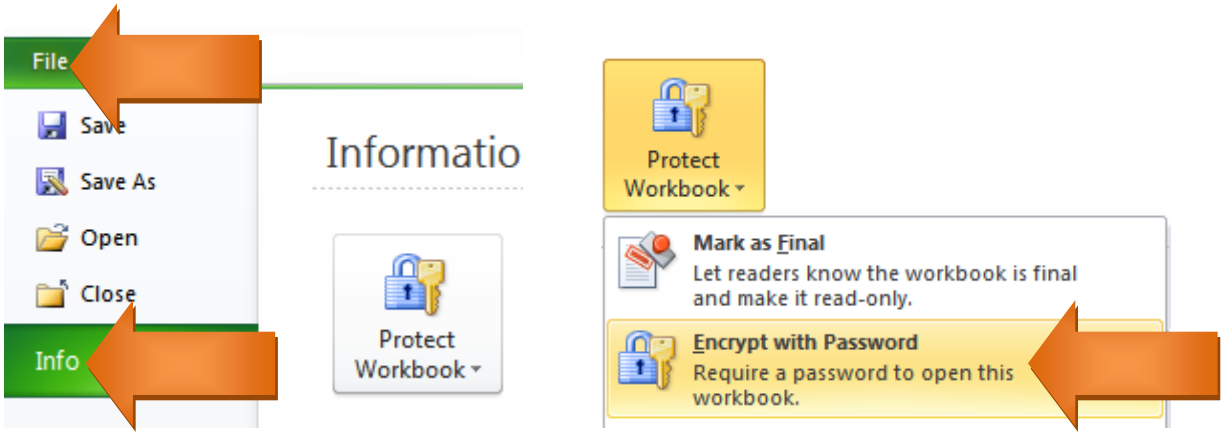
Alternatively, a word document can also be protected when sharing on a wider scale. To use this type of protection simply click on file and save as. In the bottom right hand corner, click on tools then general options. A new window will pop up.



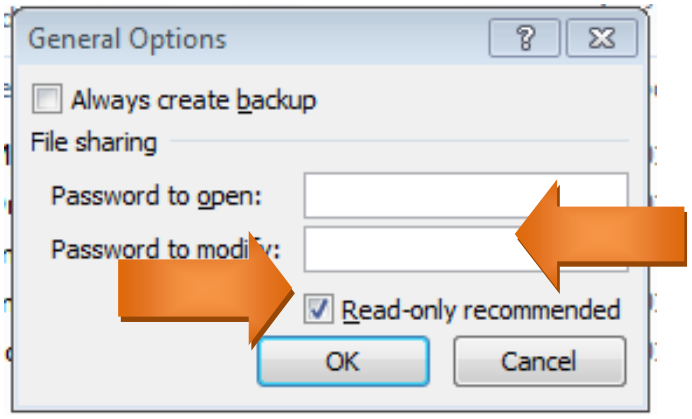
Click on OK when finished.

In Microsoft Excel 2010

Go To File / Info / Tools / Protect Workbook / Select Encrypt with Password. This is the same as in Word.



Alternatively, an excel document can also be protected when sharing on a wider scale. To use this type of protection simply click on file and save as. In the bottom right hand corner, click on tools then general options. A new window will pop up.



Click on OK when finished.

Annex D – How to Scan USB Drives / CDs / DVDs, etc.

1) Insert Device
2) Go to Start / Computer / Right Click on Device Icon / Select Scan for Virus…
3) Another window will open. It will run through the scans and let you know once complete. Allow process to finish before opening any documents from the device.

Annex E – Threat Telephone Checklist

Questions to ask:

(For Bomb Threats - What time will the bomb explode?) For other threats, what will it do?
Where is it?
What does it look like?
Where are you calling from?
Why did you place the bomb or other object?
What is your name?

Identifying characteristics of the caller:

Sex:	Male	Female	Not sure	
Estimated age (specify):				
Accent:	English	French	Other	
Voice:	Loud	Soft	Other	
Speech:	Fast	Slow	Other	
Diction:	Good	Nasal	Lisp	Other
Manner:	Emotional	Calm	Vulgar	Other
Background noise: (specify)				
Voice was familiar: (specify)				
Caller was familiar with the area: (specify)				

EXACT WORDING OF THREAT:

_____

_____

_____

Date: _____ Time:_____

Duration of Call: _____

ANNEX F – BOMB THREAT POSTER

Annex G – Quick Reference Guide to documents

	Protected A	Protected B	Protected C	Confidential	Secret	Top Secret
Security Screening Level	Reliability Status	Reliability Status	Reliability Status	Confidential Clearance (Level l)	Secret Clearance (Level ll)	Top Secret Clearance (Level lll)
Marking	Upper Right Corner if sent Outside of Office (see mailing)	Upper Right Corner of each page	Upper Right Corner of each page	Upper Right Corner of each page	Upper Right Corner of each page	Upper Right Corner of each page
Paper Storage	Locked Office or Container with keyed lock	Approved Security Cabinet with dial combination lock or approved padlock	Approved Security Cabinet for Protected C storage based on the Security Equipment Guide	Approved Security Cabinet for Confidential storage based on the Security Equipment Guide	Approved Security Cabinet for Secret storage based on the Security Equipment Guide	Approved Security Cabinet for Top Secret storage based on the Security Equipment Guide with integral combination locks
Electronic Media Storage	Shared Office drives and folders. Portable media (CD, disk, USB) labeled and with limited access.	Shared Office drives and folders. Portable media (CD, disk, USB) labeled with limited access and password protected.	Portable media (CD, disk, USB) labeled and locked up when not in use same as paper storage requirements and password protected.	Portable media (CD, disk, USB) labeled and locked up when not in use same as paper storage requirements and password protected.	Portable media (CD, disk, USB) labeled and locked up when not in use same as paper storage requirements and password protected.	Portable media (CD, disk, USB) labeled and locked up when not in use same as paper storage requirements and password protected.
Electronic Transmission	Internal Office network – System A or B	Internal Office network – PKI	No electronic transmission	Internal Office network – PKI	No electronic transmission	No electronic transmission
Fax	Regular fax	Regular fax	No Faxing	No Faxing	No Faxing	No faxing
Telephone	LAN Line (regular telephone)	LAN Line (regular telephone)	STU III – See USS	LAN Line (regular telephone)	STU III – See USS	STU III – See USS
Destruction	Machine Shred	Machine Shred	Machine Shred	Machine Shred	Machine Shred	Machine Shred
Packaging	1 gum-sealed	1 gum-sealed	2 gum-sealed	Except for delivery	Except for delivery	2 gum-sealed

	Protected A	Protected B	Protected C	Confidential	Secret	Top Secret
	envelope or single sealed wrap/box. No security marking. Within Office: economy envelope or labeled folder is acceptable.	envelope or single sealed wrap/box. No security marking. Within Office: economy envelope or labeled folder is acceptable.	envelopes. Double-sealed wrapping of bulky or heavy packages. Address on both. Security marking and To be opened only by on inner envelope or wrap. Record must be kept of documents sent.	outside Canada (see below): 1 gum-sealed envelope or single sealed wrap/box. No security marking. Within Office: economy envelope or labeled folder is acceptable.	outside Canada (see below): 1 gum-sealed envelope or single sealed wrap/box. No security marking. Within Office: economy envelope or labeled folder is acceptable.	envelopes. Double-sealed wrapping of bulky or heavy packages. Address on both. Security marking and To be opened only by on inner envelope or wrap. Record must be kept of documents sent.
In Office Delivery	Internal mail	Internal mail	Hand delivered in a sealed envelope	Internal mail in a sealed envelope	Internal mail in a sealed envelope	Hand delivered in a sealed envelope
Mailing	Within NCR 1st class mail Other Cities in Canada 1st class mail Outside Canada First class mail or reliable commercial courier.	Within NCR 1st class mail Other Cities in Canada 1st class mail Outside Canada First class mail or reliable commercial courier.	Within NCR Messengers with a Reliability Status; must use an approved briefcase for deliveries to, and from Office facilities. Other Cities in Canada Registered Mail Outside Canada Diplomatic	Within NCR Messengers cleared to Confidential; must use an approved briefcase for deliveries to, and from Office facilities. First class mail may be used in a double envelope with security marking and To be opened only by on inner envelope or wrap. Record must be kept of	Within NCR Messengers cleared to Secret; must use an approved briefcase for deliveries to, and from Office facilities. First class mail may be used in a double envelope with security marking and To be opened only by on inner	Within NCR Messengers with a Top Secret clearance; must use an approved briefcase for deliveries to, and from Office facilities. Other Cities in Canada Registered Mail Outside Canada Diplomatic Security Mail Service.

	Protected A	Protected B	Protected C	Confidential	Secret	Top Secret
			Security Mail Service. Address outer envelope to Distribution Services Division (SBG), DFAIT. Exact destination address and security marking must appear only on the inner envelope. Place a "Transmittal Note and Receipt" form (GC 44) in inner envelope. Seal inner envelope (or wrap) with approved security tape.	documents sent. <u>Other Cities in Canada</u> Confidential - First class mail with recorded transit and delivery or by reliable commercial courier <u>Outside Canada</u> Packaging and delivery same as for TOP SECRET.	envelope or wrap. Record must be kept of documents sent. <u>Other Cities in Canada</u> Secret – reliable commercial courier with recorded transit and delivery <u>Outside Canada</u> Packaging and delivery same as for TOP SECRET.	Address outer envelope to Distribution Services Division (SBG), DFAIT. Exact destination address and security marking must appear only on the inner envelope. Place a "Transmittal Note and Receipt" form (GC 44) in inner envelope. Seal inner envelope (or wrap) with approved security tape.
Hand Carried	In Briefcase tagged with return Office address	In approved Briefcase tagged with return Office address	In approved Briefcase tagged with return Office address	In approved Briefcase tagged with return Office address	In approved Briefcase tagged with return Office address	In approved Briefcase tagged with return Office address

Annex H – Roll-Call Procedures

It is necessary for the Office of the Ombudsman to put in place a means to account for all employees at the time of an evacuation.

At the onset of a crisis, employees, clients and guests are obligated to vacate the premises. When this occurs, more often than not, we get separated from our colleagues. The following procedure is being adopted by the Office of the Ombudsman to enable us to ensure that everyone for whom we are responsible has successfully exited the building without incident.

Procedures

1. Upon leaving the building, go immediately to the World Exchange Plaza located at the corner of Metcalfe and Albert Streets, one block north of our building (100 Metcalfe). There are many entrances to the World Exchange Plaza, but we recommend using the Metcalfe entrance.

2. Once you have entered the World Exchange Plaza, you are asked to look for the individual wearing a high visual yellow construction style vest. This person will be next the Metcalfe entrance. You are asked to report to this person, so that you are listed and accounted for. At the same time, Managers will be assembled in the vicinity to acknowledge any absenteeism from their team, to meet with staff and to provide them with updates and/or instructions.

3. It is the responsibility of each employee to follow these steps in an evacuation or test drill.

Annex I – Security Checks

As noted in section 3.15 of the security handbook, all employees of the Office of the Ombudsman are subject to security checks.

Either the Unit Security Supervisor or a designated Manager can randomly complete these checks after working hours. No notice will be given before a check takes place.

Spot checks may be completed during working hours if information is received that would warrant such an event. The clean desk policy as noted in section 3.6.1 should be followed during working hours.

During the silent hour checks, those conducting a security check will be looking for in particular:

- Failure to store sensitive information,
- Filing cabinets left unlocked,
- Computers not properly logged off,
- Shredding left in the open,
- Discarded classified or protected B documents in the recycling bins,
- Keys not properly secured (i.e. hidden in cubicle walls or pen holders) and
- Outgoing mail left in outboxes.
- **Attractive items left out and unsecured, i.e. BlackBerry, digital recorders, laptops, USB sticks, PKI cards etc.**

Material found on Protected B printers will be removed and shredded.

A closed office door is acceptable as a temporary means for securing protected B documents or lower during working hours. During after hour inspections, closed doors will be checked to ensure that they are locked. Unlocked offices will be subject to the same security check as cubicles. A closed door is not a permanent substitute for an approved filing cabinet.

The security checks to be conducted will be visual in nature. The office or cubicle will be entered and visually scanned for infractions. Pen/paperclip holders and cubicle wall panels will be inspected to look for keys. **Where it comes to the issue of hidden keys, we are not condoning key hiding. In actual fact, keys should not be hidden at any time, they should be securely stored or remain with the owner.** Recycling bins will be inspected for discarded classified information. Pedestals will be opened if left unlocked. It needs to be understood that all files are to be locked in the appropriate, approved filing cabinets. Please note that overhead bins or pedestals are not approved storage containers for classified or protected documents.

Annex J – Standardized Signature Blocks

The following are mandatory requirements in accordance with Treasury Board policy Appendix E: Email Signature Blocks
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27600.
Note that Office policy and discretionary items are listed and explained afterward.

Mandatory Requirements:

The Common Look and Feel (CLF) requires that the Federal Identity Program (FIP) policy, and the Official Languages policy, be followed.

- Text is to be black font on white background.
- The following fonts are acceptable: Sans-Serif font style, such as Verdana, Calibri or Arial
- Font size is 10 points
- The signature may not be in cursive form but must be typewritten to accommodate the needs of the visually impaired.
- All email messages sent by government employees to non-Government of Canada recipients must include a signature block in both official languages.
- In creating a bilingual signature, English will be listed first for offices located outside of Quebec and French will be listed first for offices located within Quebec.
- All outgoing e-mail messages sent by Government of Canada employees must include the sender's name, institution name, telephone, toll free and TTY numbers (with area code).
- The signature block must be on the same page as the end of the message (not a separate file or attachment).
- The inclusion of "Government of Canada / Government du Canada" is required for all emails.
- The same requirements are to be applied to emails on mobile devices, technology permitting.
- Do not add a building address to any signature block.

Office policy:

- Operations personnel must list the central office number (613-992-0787) and toll free numbers (1-888-828-3626) in their signature.
- Graphics and pictures (i.e.: smiley faces, emoticons, symbols, etc.) or representations of associations / organizations one belongs to (or used to belong to) are not permitted.
- Sayings, quotes, poetry or banners are not to be included anywhere in the signature block.

- Short disclaimer to be included at the end of the e-mail signature (see example at the end of this document).

Discretionary items:

- We must remain mindful of our unique position within the government as well as our arm's length relationship with DND/CAF. More specifically, we must be particularly aware of possible perception considering our constituents and their legitimate expectation for impartial treatment. For this reason, the office discourages the inclusion of former rank (for those with prior with military service), decoration notations (ie: the Canadian Forces Decoration - CD), and professional association titles or initials within the signature block.
- The abilities and achievements associated with post-secondary education are recognized by the Office but degree / certificate initials after one's name can, at times, lead to confusion (especially when the degree earned is not related to the job being done). The inclusion of academic notations in e-mail signatures, while discouraged, will be left to individual discretion.
- A link to the office website can be used in a signature block if it is for a program or service provided. You can use the universally accessible link (http://www.ombudsman.forces.gc.ca). The generic signature block is laid out in the same format as an individual's except instead of an individual's name it would be the program or service name.
- Please see your Director should you require technical assistance in creating or amending your e-mail signature.

Sample 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.

Glossary of Terms

The following is the glossary of acronyms used in this document.

BCP	Business Continuity Planning
CAF	Canadian Armed Forces
CLF	Common Look and Feel
DG	Director General
DND	Department of National Defence
FIP	Federal Identity Program
MP	Military Police
NCR	National Capital Region
PKI	Public Key Infrastructure
PRI	Personal Record Identifier
PSPC	Public Service Procurement Canada
RCMP	Royal Canadian Mounted Police
TBS	Treasury Board Secretariat
USS	Unit Security Supervisor