Information Sensitivity Toolkit

Version 1

24 February 2010

Contacts:

Archives and Records Management Section, DM (arms@un.org)
Peacekeeping Information Management Unit, DPKO (peacekeeping-imu@un.org)

Contents

1. INTRODUCTION

Records and information are important assets of the United Nations, and sound procedures for information sensitivity and security are important prerequisites for the proper management of the Organization's records. Information sensitivity relates to the level of confidentiality of the information within the United Nations. The appropriate handling of sensitive information is critical to the success of the Organization and its operations throughout the world. Information security relates to the protection of the information, including access controls. Information security also ensures that the information is available when needed and that its integrity is maintained, i.e., that it is not altered or inappropriately disclosed.

Information sensitivity and security are often extremely difficult to manage even under the best conditions, particularly in light of recent increases in both electronic information and the demand for instantaneous access to this information. These challenges are magnified within peacekeeping operations due to the unique nature of each mission and the exceptional circumstances in which they operate. Nevertheless, the need for and requirements related to managing sensitive information are not dismissed because of these challenges.

It is necessary that all staff members are aware of their responsibilities to protect records and information. The Secretary-General's Bulletin ST/SGB/2007/6 on information sensitivity, classification and handling establishes baseline United Nations policy and responsibilities on these matters. This Information Sensitivity Toolkit, used in conjunction with training, provides the requirements and means for staff members to manage sensitive records to ensure protection of the confidentiality and integrity of information contained therein, thereby meeting the requirements of ST/SGB/2007/6. The proper handling and protection of sensitive records will ensure that unauthorized disclosures are averted, thereby protecting operational integrity and the safety of staff members, United Nations partners, and local populations.

This toolkit provides easy to understand guidance on a number of topics relating to information sensitivity and security, including:

- United Nations security classification principles and levels,
- When and who classifies information,
- How to mark sensitive information,
- The requirements for access to information,
- The handling of sensitive information, and
- The downgrading, declassification and destruction of sensitive information.

a. Navigating this Toolkit

The Contents section at the beginning of this toolkit provides links to the different toolkit sections. The toolkit is designed to follow the steps required to handle and manage sensitive information in the order that they would normally occur. Links are included to printable versions of sections or requirements.

Information Boxes are provided throughout the toolkit to highlight things to remember, key points and common questions. Each type of information box has a unique picture label to identify it:

Things to remember are identified by a check list.

Key points are identified by an exclamation point.

Questions are identified by a question mark.

Answers to questions are accessed by clicking on this icon.

Where applicable, annexes of samples, checklists and templates are provided. Case studies and frequently asked questions are also included at the end of the toolkit. For example, Annex 1, "Main Things to Remember about Managing Sensitive Information" provides the core principles of this toolkit for easy reference. Please note that examples and samples are provided solely for instructional purposes because peacekeeping missions vary greatly from one to another.

If you have questions on this toolkit or on the handling of sensitive information, please contact your mission's Information Management Officer; the Peacekeeping Information Management Unit, Department of Peacekeeping Operations at UNHQ; or the Archives and Records Management Section, Department of Management at UNHQ.

2. SCOPE

This toolkit applies to all records, regardless of format, created or collected by the following operations:

- All United Nations peacekeeping operations led by the Department of Peacekeeping Operations (DPKO);
- All United Nations political operations led by the Department of Peacekeeping Operations; and
- All United Nations field support operations led by the Department of Field Support (DFS).

When the term *information* is used in this toolkit, it refers to information as contained in business records. Security of structured data in information systems is not explicitly covered in this toolkit; nevertheless,

some of the concepts covered by the toolkit may be of relevance to IT professionals in the design and maintenance of such systems.

As information security is everyone's responsibility, this toolkit is intended for use by all national and international staff members of the above operations, irrespective of the staff member's level, functional responsibility or contractual status. The toolkit also is designed for use by experts on mission, troop contingents and formed police units.

Additionally, this toolkit will be of value to special political missions led by the Department of Political Affairs (DPA) and to DPKO, DFS and DPA offices and divisions at United Nations Headquarters.

3. CLASSIFICATION PRINCIPLES

Classification is the act or process by which information is determined to be sensitive or non-sensitive. Classifying information properly is one of the core components of information security. Per ST/SGB/2007/6, the three official United Nations security classifications are: STRICTLY CONFIDENTIAL, CONFIDENTIAL and UNCLASSIFIED. The overall approach to classifying information within the United Nations is that work should be open and transparent to the extent appropriate based on the sensitivity of the information. Accordingly, information should only be classified as STRICTLY CONFIDENTIAL or CONFIDENTIAL where disclosure would be detrimental to the proper functioning of the United Nations, endanger the welfare and safety of its staff or third parties, or violate legal obligations.

Classification refers to the act or process of *determining* the sensitivity (or non-sensitivity) of information; classification does not equate to sensitivity

Information deemed sensitive, and thereby requiring a classification of STRICTLY CONFIDENTIAL or CONFIDENTIAL shall include:

a. Documents [and records] created by the United Nations, received from or sent to third parties under an expectation of confidentiality;
b. Documents [and records] whose disclosure is likely to endanger the safety or security of any individual, violate his or her rights or invade his or her privacy;
c. Documents [and records] whose disclosure is likely to endanger the security of Member States or prejudice the security or proper conduct of any operation or activity of the United Nations, including any of its peacekeeping operations;
d. Documents [and records] covered by legal privilege or related to internal investigations;
e. Internal inter-office or intra-office documents [and records], including drafts, if disclosure would undermine the Organization's free and independent decision-making process;
f. Documents [and records] containing commercial information, if disclosure would harm either the financial interests of the United Nations or those of other parties involved;
g. Other kinds of information, which because of their content or the circumstance of their creation or communication must be deemed confidential.

Source: ST/SGB/2007/6 Section 1.2

In contrast, information not meeting one or more of the above criteria should be considered as UNCLASSIFIED (if it is internal information) or PUBLIC (if it is for public consumption). The classifications are described in detail in the next section.

In the interest of organizational transparency, the security classifications STRICTLY CONFIDENTIAL and CONFIDENTIAL should be used as sparingly as possible.

4. CLASSIFICATION LEVELS

The classification principles mentioned in the previous section draw a basic distinction between sensitive information (which requires a marking of STRICTLY CONFIDENTIAL or CONFIDENTIAL) and non-sensitive yet internal information (which justifies a marking of UNCLASSIFIED).

To draw a further distinction between STRICTLY CONFIDENTIAL, CONFIDENTIAL and UNCLASSIFIED, one must also look at the degree of sensitivity of the information at hand.

Definitions of the three security classifications are as follows:

- STRICTLY CONFIDENTIAL:
  - Is the highest level of sensitivity and applies to information or material whose unauthorized disclosure could reasonably be expected to cause EXCEPTIONALLY GRAVE DAMAGE TO or IMPEDE THE CONDUCT OF THE WORK of the United Nations.

- CONFIDENTIAL:
  - Applies to information or material whose unauthorized disclosure could reasonably be expected to cause DAMAGE TO THE WORK of the United Nations.

- UNCLASSIFIED:
  - Applies to information or material whose unauthorized disclosure could reasonably be expected NOT TO CAUSE DAMAGE TO THE WORK of the United Nations.

Source: ST/SGB/2007/6 Section 2

United Nations Classification Levels are:
- ✓ STRICTLY CONFIDENTIAL
- ✓ CONFIDENTIAL
- ✓ UNCLASSIFIED

The appropriate classification level is determined by the disclosure risks of the information, which usually are identified by the magnitude, amount or kind of damage that could be caused by disclosure. Referencing the definitions above, the four types of possible damage are:

- EXCEPTIONALLY GRAVE DAMAGE TO the United Nations:
  - Definition: Irreparable harm to the United Nations, its Member States or individuals.
  - Examples: Records whose disclosure is likely to endanger the safety or security of any individual, violate his or her rights or invade his or her privacy.
    - Death or physical injury of a United Nations staff member or third party such as military contingent, police officer or citizen of a local population.
    - Violation of a staff member's right to medical privacy.
  - Examples: Records whose disclosure is likely to endanger the security of Member States or prejudice the security or proper conduct of any operation or activity of the United Nations, including any of its peacekeeping operations.

        - Troop movements within the mission area.
        - Official travel of the SRSG and VIP visit arrangements to missions.
    - Classification level of information whose disclosure could reasonably cause such damage: STRICTLY CONFIDENTIAL.

- IMPEDE[MENT TO] THE CONDUCT OF THE WORK of the United Nations:
    - Definition: Long-lasting and/or far-reaching impairment of a United Nations mission, operation or programme.
    - Examples:
        - Sabotage resulting in significant damage to a peacekeeping mission's communication channels.
        - Collapse of a local population's confidence in a peacekeeping operation.
    - Classification level of information whose disclosure could reasonably cause such damage: STRICTLY CONFIDENTIAL.

- DAMAGE TO THE WORK of the United Nations:
    - Definition: Harm to the United Nations, Member States or individuals, where damages incurred could potentially be repaired through negotiation, good offices or other means.
    - Examples:
        - Strained relations between the United Nations and a non-governmental organization.
        - Lack of confidence between the United Nations and a vendor.
    - Classification level of information whose disclosure could reasonably cause such damage: CONFIDENTIAL.

- [NO] DAMAGE TO THE WORK of the United Nations:
    - Definition: No damage will occur to the United Nations, Member States or individuals.
    - Examples:
        - The media's knowledge of a principal's participation in a conference.
        - A Member State's knowledge of how its contributions to a trust fund have been used.
    - Classification level of information whose disclosure could reasonably be expected to not cause damage: UNCLASSIFIED.

It is important to distinguish UNCLASSIFIED (i.e., non-sensitive yet internal) information from PUBLIC information. Although PUBLIC is not considered a classification level, it is important to understand what constitutes PUBLIC information to be able to classify information correctly.

- PUBLIC information:
    - Definition: Information produced expressly for public consumption or that has undergone a declassification process and is now available for public use.
    - Examples:
        - Official United Nations documents marked as "Distr: General", e.g., Security Council Resolutions.
        - SRSG press statements.
        - Policies and procedures that have been posted to a peacekeeping operation's web site following a declassification process.
        - CONFIDENTIAL and UNCLASSIFIED business records greater than 20 years old.[1]

A table detailing the differences between the security classifications is provided in Annex 2.

[1] Under United Nations standard operating procedure for records and archives, the official copy of business records will have been transferred from a mission to United Nations Headquarters long before the 20-year mark.

Unclassified information is **not** equivalent to public information.

How does one classify personal information?

5. WHEN TO CLASSIFY

Internally-drafted documents should be classified as soon as the information contained therein is determined to be sensitive.

Sensitive records received from third parties should be classified immediately upon receipt.

All records must be classified before transmission or storage to ensure that the information is handled in the appropriate manner for its sensitivity level.

Information contained in documents can be considered sensitive even if the documents have not yet been formally approved or signed as records; a security classification of STRICTLY CONFIDENTIAL or CONFIDENTIAL would be required.

6. WHO SHOULD CLASSIFY

In accordance with ST/SGB/2007/6, the drafter of the information concerned, or its recipient if the information is received from an outside source, under the overall supervision and guidance of the head of mission or mission pillar, shall decide whether the information is sensitive or not and mark it with the appropriate classification of STRICTLY CONFIDENTIAL, CONFIDENTIAL or UNCLASSIFIED.

The approver or signatory of records, under the overall supervision and guidance of the head of mission or mission pillar, reserves the right to upgrade (e.g., change UNCLASSIFIED to CONFIDENTIAL) or downgrade (e.g., change CONFIDENTIAL to UNCLASSIFIED) a security classification originally applied by a drafter.

Only staff members provided with original classification authority[2] or those staff members who have been duly designated[3] by a staff member with original classification authority within the United Nations have authority to classify information as STRICTLY CONFIDENTIAL or CONFIDENTIAL.

[2] An individual authorized in writing, either by the Head of Mission, or by section chiefs or other officials designated by the Head of Mission, to classify information in the first instance.
[3] Please see UN Secretariat form P.86 for delegation of authority. [Link: http://iseek.un.org/LibraryUNforms/524-20040614143001522015 5.doc]

Original classification authority is determined on a mission-by-mission basis, under the overall authority of the Head of Mission. An example of a possible original classification authority list is provided in Annex 3.

Note: all routine, personal information explicitly linked to staff member names or other data which would render the staff member identifiable (personal history profiles, time and attendance reports, medical leave certificates, etc.) are to be classified and marked as STRICTLY CONFIDENTIAL and handled accordingly. Therefore, all staff members handling personal information should exceptionally be granted STRICTLY CONFIDENTIAL original classification authority for this specific type of material. Refer to FAQ 24 for more information.

Possessing original classification authority does not mean that a staff member has unrestricted access to all STRICTLY CONFIDENTIAL and/or CONFIDENTIAL information. Access to information must always be based on sound access principles, which are covered in Section 9, Access to Active Records.

Original classification authority is **not** required to classify information as UNCLASSIFIED.

7. HOW TO CLASSIFY

When classifying records, care needs to be taken to ensure that the security classification accurately reflects the highest level of sensitivity found therein. It is also important to confirm whether or not the record was previously classified by an office of the United Nations or an external source. The steps to follow when classifying records apply to all records produced by the United Nations or received from an external source.

Per ST/SGB/2007/6, where information from an external source contains prior sensitivity markings, it shall retain those markings or shall be assigned a United Nations classification that provides a degree of protection greater than or equal to that of the entity that furnished the information. Assigning a United Nations classification is preferred, provided that all original classification authorities working with a particular third party are familiar with the third party's security classifications. A chart comparing United Nations classifications with those of some United Nations partners may be found in Annex 4.

The classification process is not an easy one and should not be taken lightly. Not only must the original classification authority determine a record's degree of sensitivity, but also, if at all possible, the authority should attempt to identify and record any downgrading or declassification action(s) that could occur upon the passing of a particular date or event. For example, an SRSG's travel itinerary could simultaneously be marked as STRICTLY CONFIDENTIAL and be marked for declassification immediately upon his or her return to mission headquarters.

Do I need to follow all the steps for classifying information?

The following is practical guidance on classifying information that is either being drafted internally or is received from another United Nations office or an external source. A graphic representation of these steps may be found in Annex 5, and a checklist of these concepts (for quick reference) may be found in Annex 6.

Classifying Information: The Main Steps

- **Step 1: Is the information already classified by a United Nations office?**
    - Yes:
        - Proceed to Step 1.1.
    - No
        - Proceed to Step 2.
- **Step 1.1: Does the information appear to be classified correctly?**
    - Yes:
        - Follow normal information handling procedures for the security classification.

    - No:
        - Contact the originating office to confirm the security classification.
        - Change the security classification as required.
        - Follow normal information handling procedures for the current security classification.

- **Step 2: Is the information already classified by an external source?**
    - Yes:
        - Verify which United Nations security classification would apply using the Comparison Chart for Classifying Externally Classified Records. If the external source is not listed in the chart, consult a staff member with original classification authority.
        - With the approval of the original classification authority, mark the information with a United Nations security classification equal to or higher than the external source's security classification.
        - Follow normal information handling procedures for the United Nations security classification.

    - No:
        - Proceed to Step 3.
- **Step 3: Is the information publicly available?**
    - Yes:
        - The information does not need to be classified or marked.
        - Freely transmit and share.

    - No:
        - Proceed to Step 4.
- **Step 4: Would unauthorized disclosure of the information reasonably cause damage to the United Nations, its Member States or individuals?**
    - Yes:
        - Proceed to Step 5.

- No:
  - Mark the information as UNCLASSIFIED.
  - Proceed to Step 8.

- **Step 5: Would unauthorized disclosure of the information reasonably be expected to cause exceptionally grave damage to or impede the work of the United Nations, its Member States or individuals?**

  - Yes:
    - Mark the information as STRICTLY CONFIDENTIAL.
    - Proceed to Step 7.
  - No:
    - Proceed to Step 6.

- **Step 6: Could unauthorized disclosure of the information after 20 years reasonably be expected to cause damage to the United Nations, its Member States, individuals or their families?**

  - Yes:
    - Mark the information as STRICTLY CONFIDENTIAL.
    - Proceed to Step 7.
  - No:
    - Mark the information as CONFIDENTIAL.
    - Proceed to Step 7.

- **Step 7: Is there an event or date that will automatically trigger a downgrading of the information's sensitivity?**

  - Yes:
    - On the information itself and in an electronic or paper Sensitive Records Register:
      - Note the event or date that will trigger the downgrading of the information.
      - Clearly indicate that downgrading shall take effect automatically upon the event or date.
      - Indicate the new security classification that will take effect upon the event or date.
    - Proceed to Step 8.
  - No:
    - Proceed to Step 8.

- **Step 8: Is there an event or date that will automatically trigger the information's declassification** [link to Glossary - Declassification]**?**

  - Yes:
    - On the information itself and in an electronic or paper Sensitive Records Register
      - Note the event or date that will trigger declassification of the information.
      - Clearly indicate that declassification shall take effect automatically upon the event or date.
    - Follow normal information handling procedures for the current security classification.

  - No:
    - Follow normal information handling procedures for the current security classification.

You should identify any event or date that would automatically trigger the information's downgrading or declassification.

8. MARKING SENSITIVE INFORMATION

Only authorized staff members (i.e., those staff members with original classification authority) should mark records with security classifications. Refer to Section 6, Who Should Classify.

a. Why Mark Records?

There are several reasons why records need to be marked. The marking:

- Alerts the holder to the fact that the item requires protection.
- Advises the holder of the level of protection required.
- Shows what is classified and what is not.

What is the difference between classification and marking?

b. Marking Records

Records should be marked for the highest level of security classification of the information contained therein. The entire record will be marked for the highest level of sensitive information. The following basic marking requirements should be used on all records with a security classification of STRICTLY CONFIDENTIAL, CONFIDENTIAL or UNCLASSIFIED. Wherever possible, electronic templates containing these three options should be used in the drafting process.

A record's marking must reflect the highest level of sensitivity found in any part of the record's contents.

The following pages contain requirements for marking information and for marking containers such as file folders and removable electronic media.

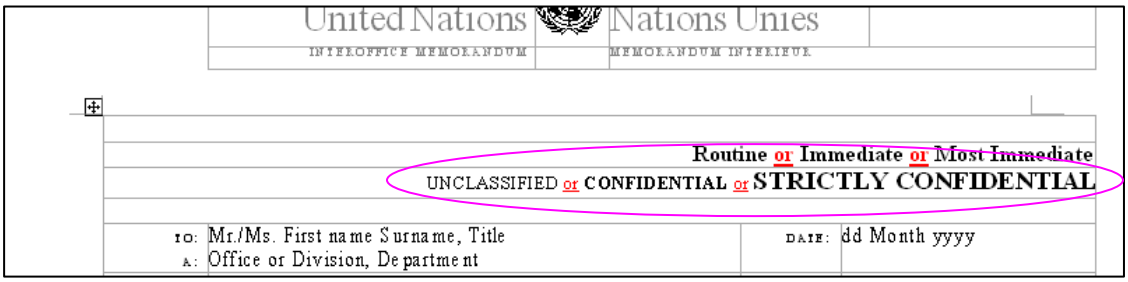
c. Marking Paper Records

Paper records are the easiest to mark. All sensitive records must be marked with the security classification of STRICTLY CONFIDENTIAL or CONFIDENTIAL; other internal records should be marked as UNCLASSIFIED. It is the responsibility of the staff member assigning the classification level to ensure that the record is appropriately marked. Listed below are the basic marking requirements for United

Nations internal information. These requirements also apply to information received from external sources that have a sensitivity marking from that source.

Basic Marking Requirements:

- The classification is NOT abbreviated: use STRICTLY CONFIDENTIAL, CONFIDENTIAL or UNCLASSIFIED.
- The marking shall be in all uppercase letters.
- The marking shall be located at the top of EACH page including all internal pages, front covers or title pages.
- The marking shall also be located at the top of the back of the last page for booklets or bound material.
- If information contains different classification levels, use the highest classification for marking the information.
- Wherever possible, use templates with security classifications, such as in the graphic below.



Specific Marking Requirements for Each Classification Level:

In addition to the basic marking requirements for paper records, specific marking requirements for each classification level are:

- STRICTLY CONFIDENTIAL will be typed or stamped in BOLD uppercase letters larger than the font size of the record.
  Example: **STRICTLY CONFIDENTIAL**

- CONFIDENTIAL will be typed or stamped in BOLD uppercase letters in the same font size as the print of the record.
  Example: **CONFIDENTIAL**

- UNCLASSIFIED should be typed or stamped in uppercase letters in the same font size as the print of the record.
  Example: UNCLASSIFIED

In addition to electronic templates, ink stamps will be required throughout the mission area. A single mission office should be assigned with establishing and promulgating stamp specifications based on the above requirements.

Specific Marking Requirements for Code Cables:

In order to simultaneously comply with the policy set forth in ST/SGB/2007/6 and the code cable procedure set forth by the Executive Office of the Secretary-General, DPKO, DFS and all DPKO- and

DFS-led missions must mark code cables in one of three ways to denote both the cable's sensitivity and its dissemination instruction:

UNCLASSIFIED
ONLY/CONFIDENTIAL
NO DISTRIBUTION/STRICTLY CONFIDENTIAL

Code cables security classified as UNCLASSIFIED **may not** bear the dissemination label ONLY or NO DISTRIBUTION. Code cables security classified as CONFIDENTIAL **must also** bear the dissemination label ONLY. Code cables security classified as STRICTLY CONFIDENTIAL **must also** bear the dissemination label NO DISTRIBUTION.

For more information, consult DPKO and DFS Circular Cable 1310 (6 June 2008): Marking code cables for sensitivity and dissemination.

d. Marking File Folders

If sensitive paper records or other media are filed within folders, the folders must also be marked with the appropriate security classification. The folder will be marked for the highest level of security classification of the information contained therein. It is the responsibility of the staff member filing the records or media to ensure that the folder is appropriately marked.

Original classification authority is **not** required to mark file folders that contain sensitive information; all staff who handle sensitive records may mark the file folders or equivalent containers

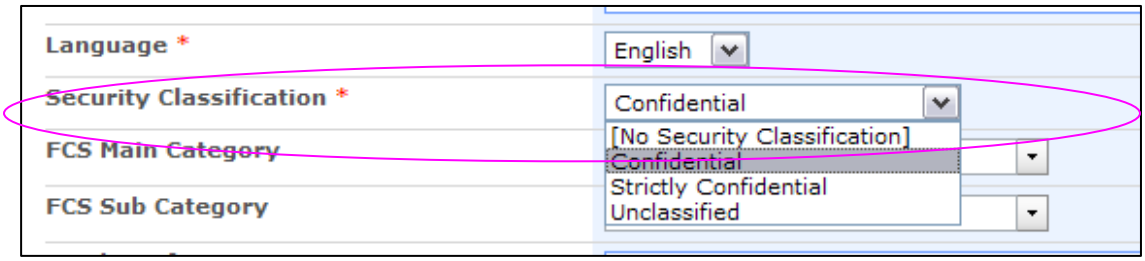
Basic Marking Requirements for File Folders:

- The classification is NOT abbreviated: use STRICTLY CONFIDENTIAL, CONFIDENTIAL or UNCLASSIFIED.
- The marking shall be in all uppercase letters.
- The marking shall appear on both sides of the file folder.

e. Marking Electronic Records

Due to the differences in electronic systems and applications, prudent judgment must be exercised in the marking of electronic records.

- In many systems, a metadata field is available during the record registration process, which enables a user to select a value of UNCLASSIFIED, CONFIDENTIAL or STRICTLY CONFIDENTIAL.



- If a system or application you are using does not have a mechanism for security classifications, consult your mission's Information Management Officer to determine the best method to mark the sensitivity level of the records contained therein.
- In exceptional circumstances where email is used to transmit sensitive information, do NOT mark the information with a security classification, as this may bring unnecessary attention to the information. If the email is printed or captured in an electronic recordkeeping system, the copy must be marked in accordance with Sections 8c or 8e, respectively, and in consultation with the originator. For additional information on the email transmission of sensitive information, refer to Section 10d.

Do NOT mark email with a security classification unless it has been captured in an electronic recordkeeping system or printed.

f. Marking Removable Electronic Media Excluding Laptop Computers

Removable electronic media (e.g. thumb drives, CDs, DVDs, external hard drives) need not be physically marked to show the highest level of classified information contained therein. If there is a need to transmit the media through the United Nations mail and pouch service or a colleague, simply place it in a double-sealed envelope, with the internal envelope bearing the appropriate marking in capital letters.

9. ACCESS TO ACTIVE RECORDS[4]

The overall approach to records access in the United Nations is based on the understanding that the work of the United Nations should be open and transparent. Internally, the vast majority of peacekeeping records should be accessible to all United Nations staff members who may benefit either directly or indirectly from the information contained therein. In contrast, a small set of sensitive records may require greater access restrictions. These records would only be accessible to colleagues and United Nations partners with a distinct need to know or right to know the information in order to perform their official functions. In this toolkit section, three distinct – yet complementary – access principles that highlight the above concepts will be discussed: need to share, need to know, and right to know.

a. Need to Share

'Need to share' is the individual and collective obligation to make records available, discoverable and accessible for colleagues that require the information to perform their official tasks. The concept of need to share also extends to providing colleagues access to information for the purpose of knowledge sharing. Such information, though not explicitly required for the colleagues' official functions, could enable them to innovate and improve by building on others' experiences and lessons learned. Need to share is a healthy baseline approach to access rights because it fosters the Organization's commitment to openness and transparency. Staff members and business units benefit greatly from a 'need to share' culture in that greater awareness of the work of others can lead to the identification of partnership opportunities, the removal of duplicative processes and documentation, and a greater ability to find information for oneself or on behalf of others. The concept of need to share can be applied to non-sensitive and sensitive records alike.

[4] Access to inactive records (i.e. records stored in an offsite facility and managed by records management professionals) involves a number of additional steps that are outside the scope of this toolkit. For guidance on access to inactive records, consult the DPKO-DFS SOP "Access and declassification of archives and non-current records".

A security alert to all staff during a crisis situation is a classic example of need to share. Other example records that one may 'need to share' include, but are by no means limited to, the following:

Broadcast Code Cables

Prior to 6 June 2008, all code cables – even if they were administrative in nature – were considered as sensitive and handled as such, resulting in highly restricted access controls in most missions and at United Nations Headquarters. As of 6 June 2008, all cables are to be marked as UNCLASSIFIED, ONLY/CONFIDENTIAL or NO DISTRIBUTION/STRICTLY CONFIDENTIAL, thereby drawing a distinction between non-sensitive and sensitive cable traffic. A good percentage of the non-sensitive cables emanating from UNHQ are broadcast in nature (e.g. announcements of a new policy or event). These broadcast cables are UNCLASSIFIED, and mission business units could benefit from seeing this information (e.g. through subsequent application of a policy to their work environment or through participation in a conference). Accordingly, missions may wish to re-evaluate how such cables are distributed within the mission area.

After Action Reviews

Per the DPKO Policy Directive on Knowledge Sharing (1 May 2009):

> An After Action Review is an analysis of an action, activity or project that allows a team to reflect on what happened, why it happened, what was learned, what follow-up action should be taken and how it can be done better in the future. Ideally, After Action Reviews should be a routine part of any action, activity or project with a view towards making recommendations for improving the efficiency and effectiveness of the organization in the future.

As can be inferred from the above, After Action Reviews are by their very nature meant to be shared.

End of Assignment Reports

Per the DPKO Policy Directive on Knowledge Sharing (1 May 2009):

> End of Assignment Reports are personal accounts by mission staff of lessons learned in the implementation of missions' mandates and on DPKO/DFS' institutional capacity to carry out mandated tasks.

Although End of Assignment Reports usually are considered sensitive, missions may choose to institutionalize the distribution of these reports to a diverse group of mission officials, even though the reports may not always relate to each official's own roles and responsibilities.

b. Need to Know

Another principle for access to records of the United Nations is 'need to know'. This concept assumes that not every staff member or person requesting access to records has the need, requirement or authority to receive the information or records. Utilizing need to know minimizes the unauthorized disclosure of sensitive information. The need to know:

- Applies primarily to sensitive records.
- **Must always be balanced with the need to share.**
- Requires that only those individuals who must have access to be able to carry out their jobs or have other strong justification for seeing the information should be provided access.
- Requires a clear delegation of authority from the originator or staff member who originally applied the classification level.
- Implies that sensitive information is only disclosed to trusted individuals to ensure that it is not widely disseminated.

Access to sensitive information is not necessarily linked to a staff member's level or grade; it is regularly linked to the staff member's functional responsibilities.

Because the establishment of 'need to know' is inherently subjective, mission offices should first establish general criteria for access to their office's business information. Only those individuals who meet the baseline criteria would be eligible for consideration. If an individual who meets these minimum standards requires a particular record, the office would then review the particular record's content vis-à-vis the individual's 'need to know' this information in order to conduct his or her official duties.

To establish baseline access criteria, sections should identify:

1. The types of business information for which they are responsible.
2. The types of staff members who require access.
3. Any restrictions to this information based on security classification.

Annex 7 provides the steps for establishing baseline access criteria and an example of how an Office of the Director of Mission Support could follow the three steps and record the resulting information in an 'access rights matrix'. The office would then use this matrix to inform its 'need to know' decisions.

An Access Rights Matrix Template may be found in Annex 8.

Staff members must use sound judgment when applying the need to know, and must always temper the need to know principle with the need to share

c. Right to Know

Under certain circumstances, United Nations staff members or offices have a 'right to know'. 'Right to know' for this toolkit refers to an individual requesting and being provided with information regarding himself/herself or information required to perform his/her job. The 'right to know' differs from 'need to know' because it applies to specific situations and, under certain circumstances, is sanctioned through approved policies.

What is meant by 'right to know'?

Responding to requests for access based on 'right to know' is simpler than determining 'need to know'. If an individual is requesting access based on the 'right to know' requirement, you should ask for the applicable requirement. If you cannot verify that the requestor has a 'right to know' and 'need to know' would not apply, you should consult the office of origin or the office of origin's original classification authority to verify the individual is authorized to access the information.

Examples of 'right to know' are:

- A staff member shall be provided with a copy of the documentary evidence of an alleged misconduct. *Source: ST/AI/371 Section 6(b)*
- The Office of Internal Oversight Services (OIOS) shall have the right of access to all records, documents or other materials … as they consider necessary to fulfil their responsibilities. *Source: ST/SGB/273 Section 4*
- A staff member has the right to access his or her official status file. *Source: ST/AI/108 Section 2*

The three concepts of need to share, need to know, and right to know must be considered prior to the release of information. The goal is to manage sensitive information to ensure its confidentially and integrity, thereby protecting operational integrity and the safety of staff members and local populations. Simultaneously, senior management must strongly discourage the intentional hoarding of information under the pretence of information sensitivity, as this activity hinders the proper functioning of the United Nations, and is anathema to the Organization's commitment to an open and transparent work environment.

When determining access to information, remember:

- ✓ Need to share
- ✓ Need to know
- ✓ Right to know

Managers have a collective responsibility to encourage a 'need to share' culture across all mission business units.

d. Implications of Releasing Information to Unauthorized Individuals

The release of information to unauthorized individuals, also known as unauthorized disclosure, can be deliberate or inadvertent, direct or indirect, oral or written. Unauthorized disclosure can also occur when a staff member without a need to know receives or retrieves classified information.

It is the responsibility of each staff member to ensure that classified information is handled and protected appropriately for the type and level of classification. Staff members must not divulge sensitive information without authorization. Since the protection and safeguarding of information is paramount to the efficiency and effectiveness of the United Nations, unauthorized disclosure of sensitive information to third parties is identified as misconduct and can result in disciplinary action against the staff member.

For more details on United Nations misconduct and disciplinary action, refer to:

- Revised disciplinary measures and procedures (ST/AI/371);
- Staff regulations (ST/SGB/2009/6); and
- Status, basic rights and duties of United Staff Members (ST/SGB/2002/13)

Unauthorized disclosure of sensitive information to third parties is identified as misconduct.

e. Access by United Nations Staff

Sensitive Information (STRICTLY CONFIDENTIAL and CONFIDENTIAL information):

Access by United Nations staff to sensitive information is not to be provided without a clear indication that the requestor is authorized to access the information. To this extent, you should:

- Ask “why” the staff member wants to see the information or requires a copy of the record. Do not just give it to them.
- Consult the office of origin or the office of origin’s original classification authority to verify the staff member is authorized to access the information.
- Offices and sections should have criteria established that sets forth how internal access is provided for each type of information they handle.
- The main principle for access to sensitive information is a need to know:
    - Only those individuals who must have access to be able to carry out their jobs or have other strong justification for seeing the information should be given access.
    - Requires a clear delegation of authority from the originator or staff member who originally applied the classification level.
    - Implies that it is only disclosed to trusted individuals to ensure that it is not widely disseminated.

Non-Sensitive Information (UNCLASSIFIED information):

- As a general rule, UNCLASSIFIED information may be shared within the United Nations Secretariat.
- Access restrictions may be employed as required, in which case access would be granted on a need to know basis.

Generally speaking, UNCLASSIFIED information may be shared within the United Nations Secretariat.

f. Access by United Nations Partners

Although a mission’s work with United Nations partners is critical to ensure the successful fulfilment of a mission’s mandate, extra precaution must always be exercised in determining access rights of non-Secretariat personnel to internal Secretariat information.

Sensitive information (STRICTLY CONFIDENTIAL and CONFIDENTIAL information):

Access by United Nations partners to sensitive information is not to be provided without a clear indication that the individual requesting access is authorized to access the information. To this extent, you should:

- Ask “why” the individual wants to see the information or requires a copy of the record. Do not just give it to them.
- Consult the office of origin or the office of origin’s original classification authority to verify the individual is authorized to access the information.
- The main principle for access to sensitive information is a need to know:
    - Only those individuals who must have access to be able to carry out their jobs or have other strong justification for seeing the information should be given access.
    - Requires a clear delegation of authority from the originator or staff member who originally applied the classification level.
    - Implies that it is only disclosed to trusted individuals to ensure that it is not widely disseminated.

Extra precaution must always be exercised in determining access rights of non-Secretariat personnel to internal Secretariat information.

Non-Sensitive Information (UNCLASSIFIED information):

- Consult the office of origin or the office of origin's original classification authority to verify the individual is authorized to access the information.

g. Access by Non-Partner Third Parties

- Only public information may be shared.
- Active internal records – regardless of security classification or perceived sensitivity – should not be shared.
- Access by third parties to non-active records involves many additional steps that are outside of the scope of this toolkit; for guidance, consult the DPKO-DFS SOP "Access and declassification of archives and non-current records".

10. HANDLING SENSITIVE INFORMATION: GENERAL PRINCIPLES

It is the responsibility of each staff member to ensure that sensitive information is handled according to all the rules associated with each classification level to prevent the unauthorized disclosure of the information. Since there are many activities included in the handling of sensitive information, each activity is presented as a separate topic below.

Each staff member has a responsibility to handle sensitive information properly and prevent unauthorized disclosure.

a. Physical Security of Sensitive Information

The security of sensitive information includes the physical security of the information immediately upon its origination or receipt. Security includes how and where information is stored or filed, how it is handled when in use and how it is maintained while awaiting destruction.

Physical security refers to security of records and information not in electronic systems and applications.

- Any staff member who has been authorized to create and maintain sensitive information is responsible for its safekeeping including its storage in secure storage facilities when not in use.
- Sensitive information should be stored in lockable cabinets, lockable rooms or safes when not in use. All keys for lockable storage rooms or cabinets should be assigned only to staff members with the appropriate authority level and tracked to ensure that keys are not lost, misplaced or copied. Combinations to safes should only be assigned to staff members with the appropriate authority level and should be changed immediately upon any indication that the combination has

been compromised. More information can be found in the Recordkeeping Toolkit for Peacekeeping Operations.

- Sensitive records that have been removed from storage must be kept under constant surveillance by staff members with authorized access and having a need to know.
- Heads of Missions should work with the mission's Physical Security Section to establish and enforce a policy requiring offices containing sensitive information to be locked when not occupied, even if the unoccupied period is for a lunch or break.
- When records are not in use they must be protected from unauthorized view until they are returned to secured storage.
- Destruction bins are to remain locked at all times.
- Each office should institute a 'clean desk' policy which requires that no one leaves information on their desk or in offices that are not secured when the staff member leaves for an extended period of time or at the end of his or her work shift.
- Staff members should remain cognizant of persons in their offices if sensitive information is in use.
- Only authorized staff members should have access to the secured locations for sensitive information. For example, a mission's communications centre, Joint Mission Analysis Centre (JMAC) or Joint Operations Centre (JOC) should have clear access rules.
- In the absence of an electronic recordkeeping system[5], a hard copy of sensitive information received in an electronic form must be printed and marked with a security classification when received, and filed and stored in accordance with the classification level assigned.

Physical security includes:

- ✓ Storage in lockable cabinets, rooms or safes.
- ✓ Constant surveillance when in use.
- ✓ Keeping destruction bins locked.
- ✓ Instituting a 'clean desk' policy.

A 'clean desk' policy is crucial to a successful information security programme.

b. Use of Electronic Systems, Applications and Media for Sensitive Information

With more of the records originated or received by the United Nations generated and stored via electronic means, it is imperative that sensitive electronic information be handled appropriately to ensure that it is protected and safeguarded against unauthorized disclosure.

Information Systems:

- Heads of departments and offices, in cooperation with [the Office of Information and Communications Technology (OICT)],[6] shall establish procedures to ensure that automated information systems (including networks and telecommunication systems) that collect, create, communicate, compute, disseminate, process or store sensitive information have controls that

[5] For more information on what constitutes an electronic recordkeeping system, see the Recordkeeping Toolkit for Peacekeeping Operations. [link]

[6] The Office of Information and Communications Technology was created in 2009 and is mandated to assume, *inter alia*, all responsibilities previously assigned to the Information Technology Services Division in the Department of Management.

both prevent access by unauthorized persons and ensure the integrity of the information. – *Source: ST/SGB/2007/6 Section 5.4*

- In the development of IT solutions, offices/organizational units stipulate business requirements, and OICT and corresponding offices (including DFS Information and Communications Technology Division – ICTD) implement adequate information systems commensurate with the sensitivity of information that will be processed, stored or transferred by the system.
- If sensitive information is moved or transferred from one system or application to another, the access level must remain at the same level as in the original system or application.
- User access to electronic systems or applications must be periodically reviewed and the access levels differentiated to ensure staff members have the correct level of access: read-only, write access (including modify), delete and/or create.
- Access rights should be reviewed periodically and changed or terminated when a user changes positions or offices.

Who determines if an electronic system or application is safe to store, process or transmit sensitive information?

Desktop Computers:

- In the performance of their official duties, authorized users of ICT resources should only use desktop computers that are owned and managed by the United Nations, and that comply with current ICT configuration standards and guidelines.
- All desktop computers must be configured to regularly apply security updates for all installed software.
- All desktop computers must at minimum have anti-virus software installed, activated and configured to receive updates at least once daily.
- All desktops must be configured to not accept incoming connections from public Internet addresses.
- Authorized users of ICT resources shall use strong passwords in adherence with established password policy requirements and standards.
- Authorized users of ICT resources should not use the hard drive (C: drive) of their computers to store sensitive information. Sensitive information should preferably be filed in an electronic recordkeeping system. In the absence of such a system, the information should be filed on secured network drives, ideally a personal network drive (i.e. H: drive) or an appropriately protected location of a shared network drive and in accordance with departmental filing standards [link to FCS]. Contact OICT or corresponding office (your mission's Communications and Information Technology Section – CITS) to ensure you have a secured network drive available for the sensitive information.
- Only if a secured network drive (personal or shared) is not available may sensitive information be filed on the local hard drive. Under these circumstances sensitive information may also be filed on removable electronic devices such as thumb drives utilizing the appropriate handling methods identified in the next section.
- Staff members should regularly 'clean up' their computers and network locations by deleting unnecessary copies and old records which have met their retention periods.
- All desktop computers shall be configured to utilize the automatic time out/lock feature in adherence with established clear screen policy requirements.

In the absence of an electronic recordkeeping system, sensitive information:

- ✓ Should be stored on a personal network drive (i.e. H:) or an appropriately protected location of a shared network drive.
- ✓ Should NOT be stored on hard drives (C:).

How can I check my password strength?

Removable Electronic Media Including Mobile Computing Devices and Laptop Computers:

The use of removable electronic media should be kept to a minimum to prevent unauthorized disclosure of sensitive information. Since removable electronic media including thumb drives, USB drives, CDs, DVDs and laptop computers can store a large volume of information, it is imperative that sensitive information be destroyed from them when no longer required on the media (See Section 10e below). In addition, the following steps should be taken when using removable electronic media and laptop computers for sensitive information:

- Sensitive information on such media should be protected by encrypting individual files, by creating encrypted containers ("partitions") or by encrypting the entire device. In all these cases the encryption must be "strong", i.e. be based on an approved algorithm such as the "Advanced Encryption Standard" (AES).) (http://csrc.nist.gov/publications).
- In addition to using strong encryption, sensitive information that is stored on removable media must be protected by a secure authentication mechanism such as a sufficiently strong password. Removable media that use weak encryption algorithms or no encryption at all are not suitable for the storage of sensitive information, even if they utilize strong authentication mechanisms such as finger print readers or padlocks.
- Removable media are suitable for the storage of sensitive information if they are certified according to "FIPS 140-2 level 2"." (http://csrc.nist.gov/publications)
- Remember to maintain your password in a secured area for any encryption of the devices or the information will not be accessible.
- When travelling, ensure that only required sensitive information is stored on removable electronic media or laptop computers. The device or computer may be confiscated in certain situations.
- When travelling, hand-carry all removable electronic media and laptop computers. Do NOT put them into checked baggage.
- All laptops must fulfil the same requirements as desktop computers.
- All laptops shall be configured to utilize the automatic time out/lock feature in adherence with established clear screen policy requirements.

Removable Media and Laptop Computers:

- ✓ Encrypt all sensitive information.
- ✓ Only store required information.
- ✓ Hand-carry when travelling.
- ✓ Do NOT put in checked baggage.
- ✓ Do not leave removable media and laptop computers unattended in unsecured or public areas.
- ✓ Use automatic time out/lock on laptop.

c. Duplication of Sensitive Information

As with access, duplication of sensitive information should be kept to a minimum to prevent wide dissemination and the greater possibility of unauthorized disclosure or access to the information.

- Sensitive materials may be duplicated only with the authorization of either the originator or the head of the receiving or originating section or office. This approval is implicit when duplication is performed in accordance with distribution lists for materials of a recurring nature.
- Ensure only required copies are made and provided.
- Use photocopiers and printers that are either secured or attended when printing or copying sensitive information.

- If using unsecured or unattended printers and photocopiers for sensitive information, ensure that you immediately go to the printer or copier upon completing the “send” or “print” command; if available, take advantage of the printer’s or copier’s PIN features.
- Use of digital senders without enabled security features and authentication is prohibited.
- Duplication activities must be recorded in a Sensitive Records Register.

Duplication: Keep it to a minimum!

d. Transmission of Sensitive Information

Transmission of sensitive information involves any method of transmission from hand delivery to sending information via email or other electronic means. The means of transmission should be selected based on the level of sensitivity of the information at hand.

Sender of Sensitive Information Requirements:

The sender of sensitive information must:

- Establish that there is a need to share or ensure the recipient of the information has an established need to know or right to know status.
- Ensure that the sensitive information is being transferred by the most secure means possible.
- Ensure sensitive information is properly classified at the point of origin.
- Ensure that the recipient supplies a receipt for the information by either having the recipient sign, date and return a standard receipt, if one has been established, or by having the recipient sign, date and return the cover page for the document which identifies the documents transmitted.

Means of transmission is based on level of information sensitivity.

Recipient of Sensitive Information Requirements:

The recipient of sensitive information must:

- Acknowledge receipt of the information.
- Ensure that the originator has applied the appropriate classification.
- Contact the originator if the applied classification needs adjustment.
- Never change a classification without the originator’s consent.
- Document the originator’s consent alongside the copy maintained in the business unit’s paper or electronic recordkeeping system (e.g. central file).
- Ensure the appropriate handling of the information according to the level of classification.
- For sensitive information received from third parties, consult your office’s original classification authority for guidance.

Paper Record Transmission of Sensitive Information:

- Where feasible, use the United Nations pouch system.

- All sensitive information must be transported in double-sealed envelopes or containers, with only the internal envelope or container clearly marked with the classification level.
- Use the correct level of staff member for hand delivery of sensitive information.
- Whenever possible, send sensitive information on a one-to-one basis (i.e., from one person to one person rather than from one person to several people).
- Recurrent sensitive information (such as operational updates and periodic political assessments) should be distributed through established distribution lists developed by each section or office to provide an auditable system for transmission and control. The Code Cable Distribution List Template at Annex 10 and the Sample Code Cable Distribution List at Annex 11 are provided as examples. Note that code cables may include non-sensitive as well as sensitive information.
- Sensitive information must not be disseminated outside the mission area without the consent of the originating mission section, office or higher authority.
- STRICTLY CONFIDENTIAL information must be transmitted separately from information bearing lower level classifications.
- The transmittal of all outgoing and incoming sensitive information must be recorded in a Sensitive Records Register.

Paper Record Transmission:

- ✓ Use the pouch system.
- ✓ Use double-sealed envelopes or containers.
- ✓ Only mark the internal envelope or container with the security classification.
- ✓ Use distribution lists for recurrent sensitive information.
- ✓ Record actions in a sensitive records register.

Email Transmission of Sensitive Information:

Sensitive information should not be transmitted by email. However, it is understood that there may be emergency situations where sensitive information must be transmitted using this technology.

- STRICTLY CONFIDENTIAL or CONFIDENTIAL information should be transmitted as a code cable or hand delivered.
- Email generally should not be used to transmit information that is classified as STRICTLY CONFIDENTIAL or CONFIDENTIAL.
- A Section Chief (or higher) should determine when email should be used for transmitting STRICTLY CONFIDENTIAL or CONFIDENTIAL information.

When it is absolutely necessary to use email to transmit sensitive information, take the following steps, and in consultation with your mission's CITS:

- All email containing sensitive information must be encrypted.
- "Sign" email delivery option shall be enabled.
- Verify each time before sending that the email is addressed to the correct person(s).
- Verify on a regular basis that email distribution lists are correct and up-to-date.
- Send the email to as few recipients as possible.
- Do not indicate the classification level in the email itself, as this may bring unnecessary attention to the email contents.
- Delete the email from the Inbox (for recipients) or Sent folder (for senders) after the transmission as the email system is not approved to store sensitive information.
- Store the email as a print-out in a paper recordkeeping system or electronically in an electronic recordkeeping system, ensuring that the systems have adequate access controls as detailed in Sections 10a and 10b, respectively.

Email should **not** be used to transmit sensitive information.

Is it OK to email a code cable?

Fax Transmission of Sensitive Information:

Sensitive information must **never** be transmitted via fax.

e. Destruction of Sensitive Information

The final activity in safeguarding and protecting sensitive information is the actual destruction of the information or record once it is eligible for destruction.

- Official copies of sensitive mission records – as is the case with all business records – should be destroyed in accordance with the Peacekeeping and Political Operations Retention Schedule (PORS) and related procedures.
- Convenience copies of sensitive information should be destroyed when no longer needed.
- Use appropriate secure destruction methods for the media and format of the sensitive information.
- Never put sensitive information in trash bins.
- Paper records should be placed in lockable containers while awaiting destruction.

Sensitive information:

- ✓ Destroy official copies in accordance with the PORS.
- ✓ Destroy convenience copies when no longer needed.
- ✓ Use secure destruction methods.
- ✓ Never put in trash bins.

Specific information on the destruction for sensitive information in different media and formats can be found in the Recordkeeping Toolkit for Peacekeeping Operations.
Destruction of electronic records is a complex process; simply deleting data or formatting media does not reliably destroy information. Staff members should contact the mission CITS for assistance; the mission CITS should, in turn, comply with applicable guidelines provided by OICT and DFS/ICTD.

11. HANDLING SENSITIVE INFORMATION: BY CLASSIFICATION LEVEL

The specific requirements for handling sensitive information are different for each classification level. The following sections provide the handling requirements specific to each level of classification for easy reference.

Are the requirements for handling STRICTLY CONFIDENTIAL and CONFIDENTIAL information the same?

a. Handling STRICTLY CONFIDENTIAL Information

Since STRICTLY CONFIDENTIAL information has the greatest risk to the Organization if there is an unauthorized disclosure, it has the strictest handling requirements.

Access:

- Consult the office of origin or the office of origin's original classification authority to verify the individual is authorized to access the information.
- The main principle for access to STRICTLY CONFIDENTIAL information is a need to know:
    - Only those individuals who must have access to be able carry out their jobs or have other strong justification for seeing the information should be given access.
    - It is determined by the staff member processing the information, in consultation with the office of origin.
    - Requires a clear delegation of authority from the originator or staff member who originally applied the classification level.
    - Implies that it is only disclosed to trusted individuals to ensure that it is not widely disseminated.
- In extreme circumstances, need to share may also apply to STRICTLY CONFIDENTIAL information.

Physical Security:

- Filed in locked containers that are in locked rooms in areas under United Nations control.
- Keys to lockable containers and rooms must be accounted for and tracked, and issued to the absolute smallest number of staff members possible.
- Safe combinations should be assigned to the absolute smallest number of staff members possible.
- Safe combinations should be changed immediately upon any indication of compromise.
- Must be kept under constant surveillance by staff members with authorized access and having a need to know when removed from storage.
- Must be protected from unauthorized view until returned to secured storage.
- Destruction bins are to remain locked at all times.
- Maintain a 'clean desk' policy where no STRICTLY CONFIDENTIAL information is left on desks when the authorized user steps away – even for a moment.
- Staff members should remain cognizant of persons in their offices.
- In the absence of an electronic recordkeeping system, a hard copy of STRICTLY CONFIDENTIAL information received in an electronic form must be printed and marked with the STRICTLY CONFIDENTIAL security classification when received, and filed and stored in accordance with approved requirements.

Physical security includes:

- ✓ Storage in lockable cabinets, rooms or safes.
- ✓ Constant surveillance when in use.
- ✓ Keeping destruction bins locked.
- ✓ Instituting a 'clean desk' policy.

Use of Information Systems:

- Automated information systems must have controls that both prevent access by unauthorized persons and ensure the integrity of the information.
- Should maintain a record of attempted and successful access to information. Such records should be regularly reviewed for any anomalies.
- Should be maintained only in electronic systems deemed secure by the mission CITS, in consultation with DFS/ICTD and OICT.
- If STRICTLY CONFIDENTIAL information is moved or transferred from one system or application to another, the access level must be assured to remain at the same level as in the original system or application.
- User access to electronic systems or applications must be reviewed and the access levels differentiated to ensure staff members have the correct level of access: read-only, write access (including modify), delete and/or create.
- Access rights should be periodically reviewed and changed or terminated when a user changes positions or offices in adherence with the established ICT security policies and standards.

Who determines if an electronic system or application is safe to store sensitive information?

Use of Desktop Computers:

- Do not use the hard drive (C: drive) of your computer to store STRICTLY CONFIDENTIAL information.
- Utilize secured network drives, either shared or authorized user's (i.e. H:) drive (contact CITS if needed).
- 'Clean up' your computer and network locations by deleting unnecessary copies and old records which have met their retention periods.
- All desktop computers shall be configured to utilize the automatic time out/lock feature in adherence with established clear screen policy requirements.

In the absence of an electronic recordkeeping system, STRICTLY CONFIDENTIAL information:

- ✓ Should be stored on personal network (H:) drives.
- ✓ Should NOT be stored on hard (C:) drives.
- ✓ Should NOT be stored on shared drives accessible by large groups of staff members

Removable Electronic Media Including Mobile Computing Devices and Laptop Computers:

- All removable electronic media and laptop computers should be encrypted.

- When travelling, ensure that only required STRICTLY CONFIDENTIAL information is stored on removable electronic media or laptop computers.
- When travelling, hand-carry all removable electronic media and laptop computers. Do NOT put them into checked baggage.
- All laptop computers shall be configured to utilize the automatic time out/lock feature in adherence with established clear screen policy requirements.

Removable Media and Laptop Computers:

- ✓ Should be encrypted.
- ✓ Only store required information.
- ✓ Hand-carry when travelling.
- ✓ Do NOT put in checked baggage.
- ✓ Use automatic time out/lock on laptop.

Duplication:

- May be duplicated only with the authorization of either the originator or the head of the receiving or originating section or office.
- Where feasible, maintain a single consultation copy of STRICTLY CONFIDENTIAL information, rather than creating one or more convenience copies.
- Use photocopiers and printers that are either secured or attended.
- If using unsecured or unattended printers and photocopiers, ensure that you immediately go to the printer or copier upon completing the “send” or “print” command; if available, take advantage of the printer’s or copier’s PIN features.
- The duplication of STRICTLY CONFIDENTIAL information must be recorded in a Sensitive Records Register.

Prefer a single consultation copy of a STRICTLY CONFIDENTIAL record instead of creating duplicates.

Sender of STRICTLY CONFIDENTIAL Information:

- Establish that there is a need to share or ensure the recipient of the information has an established need to know or right to know status.
- Ensure that the sensitive information is being transferred by the most secure means possible.
- Ensure sensitive information is properly classified at the point of origin.
- Ensure that the recipient understands the handling requirements associated with the level of classification of the information.
- Ensure that the recipient supplies a receipt for the information.

Means of transmission is based on level of information sensitivity.

Recipient of STRICTLY CONFIDENTIAL Information:

- Acknowledge receipt of the information.
- Ensure that the originator has applied the appropriate classification.
- Contact the originator if the applied classification needs adjustment.
- Never change a classification without the originator's consent.
- Document the originator's consent alongside the copy maintained in the business unit's central file.
- Ensure the appropriate handling of the information according to the level of classification.

Paper Record Transmission:

- Where feasible, use the United Nations pouch system.
- Must be transported in double-sealed envelopes or containers, with only the internal envelope or container clearly marked with STRICTLY CONFIDENTIAL.
- Use the correct level of staff member for hand delivery; for STRICTLY CONFIDENTIAL information; where feasible, prefer personal assistants who regularly handle such information on behalf of their principals.
- Whenever possible, send STRICTLY CONFIDENTIAL information on a one-to-one basis (i.e., from one person to one person rather than from one person to several people).
- Recurrent STRICTLY CONFIDENTIAL information (such as operational updates and periodic political assessments) should be transmitted through established distribution lists developed by each section or office to provide an auditable system for transmission and control.
- Staff members must not disseminate STRICTLY CONFIDENTIAL information outside the mission area without the consent of the originating DPKO, DFS or mission office, or higher authority.
- STRICTLY CONFIDENTIAL information must be transmitted separately from information bearing lower level classifications.
- The transmittal of all outgoing and incoming STRICTLY CONFIDENTIAL information must be recorded in a Sensitive Records Register.

Paper Record Transmission:

- ✓ Use the pouch system.
- ✓ Use double-sealed envelopes or containers.
- ✓ Only mark STRICTLY CONFIDENTIAL on the internal envelope or container.
- ✓ Use distribution lists for recurrent STRICTLY CONFIDENTIAL information.
- ✓ Record actions in a sensitive records register.

Email Transmission:

- Should not be used to transmit STRICTLY CONFIDENTIAL information.
- Section Chief (or higher) should determine when email should be used for transmitting STRICTLY CONFIDENTIAL information.
- If used, email must be encrypted.
- Verify each time before sending that the email is addressed to the correct person(s).
- Verify on a regular basis that email distribution lists are correct and update as required.
- The sender and/or recipient may be required to print the email for filing and preservation of the record.
- Send the email to as few recipients as possible.
- Do not indicate classification level in the email itself.

Email should **not** be used to transmit STRICTLY CONFIDENTIAL information.

Fax Transmission:

STRICTLY CONFIDENTIAL information must **never** be transmitted via fax.

Destruction:

- Destroy in accordance with the Peacekeeping and Political Operations Retention Schedule (PORS).
- Use appropriate secure destruction methods for the media and format.
- Do not put in trash bins.
- Must be placed in lockable containers while awaiting destruction.
- Specific information on the destruction of sensitive information in different media and formats can be found in the Recordkeeping Toolkit for Peacekeeping Operations.
- Destruction of electronic records should be coordinated with the mission CITS.

STRICTLY CONFIDENTIAL information:

- ✓ Destroy official copies in accordance with the PORS.
- ✓ Destroy convenience copies when no longer needed, and no later than the official copy.
- ✓ Use secure destruction methods.
- ✓ Never put in trash bins.

A Quick Guide with reference information for marking and handling STRICTLY CONFIDENTIAL information is provided.

b. Handling CONFIDENTIAL Information

Due to the sensitivity of CONFIDENTIAL information, certain handling requirements are needed.

Access:

- Consult the office of origin or the office of the origin's original classification authority to verify the person is authorized to access the information.
- The main principle for access to CONFIDENTIAL information is a need to know:
  - Only those individuals who must have access to be able carry out their jobs or have other strong justification for seeing the information should be given access.
  - It is determined by the staff member processing the information, in consultation with the office of origin.
  - Requires a clear delegation of authority from the originator or staff member who originally applied the classification level.
  - Implies that it is only disclosed to trusted individuals to ensure that is not widely disseminated.

- Need to share may also apply to CONFIDENTIAL information.

Physical Security:

- Filed in locked containers or locked rooms in areas under United Nations control.
- Keys to lockable equipment and rooms must be accounted for and tracked.
- Safe combinations assigned only to appropriate staff members.
- Safe combinations should be changed immediately upon any indication of compromise.
- Must be kept under constant surveillance by staff members with authorized access and having a need to know when removed from storage.
- Must be protected from unauthorized view until returned to secured storage.
- Destruction bins are to remain locked at all times.
- Maintain a 'clean desk' policy where no CONFIDENTIAL information is left on desks or in offices that are not secured when staff members leave for extended periods or at the end of their work shift.
- Staff members should remain cognizant of persons in their offices.
- In the absence of an electronic recordkeeping system, a hard copy of CONFIDENTIAL information received in an electronic form must be printed and marked with the CONFIDENTIAL security classification when received, and filed and stored in accordance with approved requirements.

Physical security includes:

- ✓ Storage in lockable cabinets, rooms or safes.
- ✓ Constant surveillance when in use.
- ✓ Keeping destruction bins locked.
- ✓ Instituting a 'clean desk' policy.

Use of Information Systems:

- Automated information systems must have controls that both prevent access by unauthorized persons and ensure the integrity of the information.
- Should be maintained only in electronic systems deemed secure by the mission (CITS), in consultation with DFS/ICTD and OICT.
- If CONFIDENTIAL information is moved or transferred from one system or application to another, the access level must be assured to remain at the same level as in the original system or application.
- User access to electronic systems or applications must be reviewed and the access levels differentiated to ensure staff members have the correct level of access: read-only, write access (including modify), delete and/or create.
- Access rights should be reviewed and changed or terminated when a user changes positions or offices.

Who determines if an electronic system or application is safe to store sensitive information?

Use of Desktop Computers:

- Do not use the hard drive (C: drive) of your computer to store CONFIDENTIAL information.

- Utilize secured network drives, either shared or authorized user's (i.e. H:) drive (contact CITS if needed).
- 'Clean up' your computer and network locations by deleting unnecessary copies and old records which have met their retention periods.
- All desktop computers shall be configured to utilize the automatic time out/lock feature in adherence with established clear screen policy requirements.

In the absence of an electronic recordkeeping system, CONFIDENTIAL information:

- ✓ Should be stored on personal network (H:) drives.
- ✓ Should NOT be stored on hard (C:) drives.
- ✓ Should NOT be stored on shared drives accessible by large groups of staff members.

Removable Electronic Media Including Mobile Computing Devices and Laptop Computers:

- All removable electronic media and laptop computers should be encrypted.
- When travelling, ensure that only required CONFIDENTIAL information is stored on removable electronic media or laptop computers.
- When travelling, hand-carry all removable electronic media and laptop computers. Do NOT put them into checked baggage.
- All laptop computers shall be configured to utilize the automatic time out/lock feature in adherence with established clear screen policy requirements.

Removable Media and Laptop Computers:

- ✓ Should be encrypted.
- ✓ Only store required information.
- ✓ Hand-carry when travelling.
- ✓ Do NOT put in checked baggage.
- ✓ Use automatic time out/lock on laptop.

Duplication:

- May be duplicated only with the authorization of either the originator or the head of the receiving or originating section or office.
- Ensure only required copies are made and provided.
- Use photocopiers and printers that are either secured or attended.
- If using unsecured or unattended printers and photocopiers, ensure that you immediately go to the printer or copier upon completing the "send" or "print" command; if available, take advantage of the printer's or copier's PIN features.
- The duplication of CONFIDENTIAL information must be recorded in a Sensitive Records Register.

Duplication: Keep it to a minimum!

Sender of CONFIDENTIAL Information:

- Establish that there is a need to share or ensure the recipient of the information has an established need to know or right to know status.
- Ensure that the sensitive information is being transferred by the most secure means possible.
- Ensure sensitive information is properly classified at the point of origin.
- Ensure that the recipient understands the handling requirements associated with the level of classification of the information.
- Ensure that the recipient supplies a receipt for the information.

Means of transmission based on level of information sensitivity.

Recipient of CONFIDENTIAL Information:

- Acknowledge receipt of the information.
- Ensure that the originator has applied the appropriate classification.
- Contact the originator if the applied classification needs adjustment.
- Never change a classification without the originator's consent.
- Document the originator's consent alongside the copy maintained in the business unit's central file.
- Ensure the appropriate handling of the information according to the level of classification.

Paper Record Transmission:

- Where feasible, use the United Nations pouch system.
- Must be transported in double-sealed envelopes or containers, with only the internal envelope or container clearly marked with CONFIDENTIAL.
- Use the correct level of staff member for hand delivery; where feasible, a team member who regularly handles such information is preferred.
- Whenever possible, send CONFIDENTIAL information on a one-to-one basis (i.e., from one person to one person rather than from one person to several people).
- Recurrent CONFIDENTIAL information (such as operational updates and periodic political assessment) should be transmitted through established distribution lists developed by each department or office to provide an auditable system for transmission and control.
- The transmittal of all outgoing and incoming CONFIDENTIAL information must be recorded in a Sensitive Records Register.

Paper Record Transmission:

- ✓ Use the pouch system.
- ✓ Use double-sealed envelopes or containers.
- ✓ Only mark CONFIDENTIAL on the internal envelope or container.
- ✓ Use distribution lists for recurrent CONFIDENTIAL information.
- ✓ Record actions in a sensitive records register.

Email Transmission:

- Should not be used to transmit CONFIDENTIAL information.
- Section Chief (or higher) should determine when email should be used for transmitting CONFIDENTIAL information.
- If used, email must be encrypted.
- Verify each time before sending that the email is addressed to the correct person(s).
- Verify on a regular basis that email distribution lists are correct and update as required.
- The sender and/or recipient may be required to print the email for filing and preservation of the record.
- Send the email to as few recipients as possible.
- Do not indicate classification level in the email itself.

Email should **not** be used to transmit CONFIDENTIAL information.

Fax Transmission:

CONFIDENTIAL information must **never** be transmitted via fax.

Destruction:

- Destroy in accordance with the Peacekeeping and Political Operations Retention Schedule (PORS).
- Use appropriate secure destruction methods for the media and format.
- Do not put in trash bins.
- Should be placed in lockable containers while awaiting destruction.
- Specific information on the destruction of classified information in different media and formats can be found in the Recordkeeping Toolkit for Peacekeeping Operations.
- Destruction of electronic records should be coordinated with the mission CITS.

CONFIDENTIAL information:

- ✓ Destroy official copies in accordance with the PORS.
- ✓ Destroy convenience copies when no longer needed, and no later than the official copy.
- ✓ Use secure destruction methods.
- ✓ Never put in trash bins.

A Quick Guide with reference information for marking and handling CONFIDENTIAL information is provided.

c. Handling UNCLASSIFIED Information

UNCLASSIFIED records have the lowest classification level within the United Nations. Although these records are not considered sensitive, they should be protected from unauthorized disclosure outside the United Nations.

Access:

- Although UNCLASSIFIED information generally is unrestricted within the United Nations, a need to know may still exist for select records, in which case:
    - Only those individuals who must have access to be able to carry out their jobs or have other strong justification for seeing the information should be given access.
    - It is determined by the staff member processing the information, in consultation with the office of origin.

Physical Security:

- UNCLASSIFIED information may be filed on open shelving but the shelving must be under United Nations control.
- Only authorized staff members should have access to the locations for UNCLASSIFIED information.
- In the absence of an electronic recordkeeping system, a hard copy of UNCLASSIFIED information received in an electronic form must be printed and should be marked with UNCLASSIFIED when received, and filed and stored in accordance with requirements.

UNCLASSIFIED information:
- ✓ May be filed on open shelving.
- ✓ Only authorized staff members should have access.

Use of Information Systems:

- Automated information systems must have controls that both prevent access by unauthorized persons and ensure the integrity of the information.
- If UNCLASSIFIED information is moved or transferred from one system or application to another, the access level must be assured to remain at the same level as in the original system or application.
- User access to electronic systems or applications must be reviewed and the access levels differentiated to ensure staff members have the correct level of access: read-only, write access (including modify), delete and/or create.
- Access rights should be reviewed and changed or terminated when a user changes positions or offices.

Automated systems must have controls to prevent access by unauthorized persons and ensure integrity of the information.

Use of Desktop Computers:

- ‘Clean up’ your computer and network locations by deleting unnecessary copies and old records which have met their retention periods.
- All desktop computers shall be configured to utilize the automatic time out/lock feature in adherence with established clear screen policy requirements.

UNCLASSIFIED information:

- ✓ MAY be stored on personal network (H:) drives.
- ✓ MAY be stored on hard (C:) drives.
- ✓ MAY be stored on shared drives accessible by large groups of staff members

Removable Electronic Media including Laptop Computers:

- When travelling, ensure that only required UNCLASSIFIED information is stored on removable electronic media or laptop computers.
- When travelling, hand-carry all removable electronic media and laptop computers. Do NOT put them into checked baggage.
- All laptop computers shall be configured to utilize the automatic time out/lock feature in adherence with established clear screen policy requirements.

Removable Media and Laptop Computers:

- ✓ Should be encrypted.
- ✓ Only store required information.
- ✓ Hand-carry when travelling.
- ✓ Do NOT put in checked baggage.
- ✓ Use automatic time out/lock on laptop.

Duplication:

- Ensure only required copies are made and provided.

Paper Record Transmission:

- All staff may transmit UNCLASSIFIED information.
- Generally speaking, UNCLASSIFIED information is unrestricted within the United Nations.

Email Transmission:

- UNCLASSIFIED information may be emailed.
- Verify each time before sending that the email is addressed to the correct person(s).
- Verify on a regular basis that email distribution lists are correct and up-to-date.
- The sender and/or recipient may be required to print the email for filing and preservation of the record.
- Send the email to as few recipients as possible.

Fax Transmission:

- Fax cover sheets should always be used.
- Verify each time before sending that the recipient's fax number is correct.
- The sender and/or recipient may be required to print the fax for filing and preservation of the record.

Always use fax cover sheets.

Destruction:

- Destroy in accordance with the Peacekeeping and Political Operations Retention Schedule (PORS).
- Use appropriate destruction methods for the media and format.
- Do not put in trash bins, where possible.
- Specific information on the destruction of UNCLASSIFIED information in different media and formats can be found in the Recordkeeping Toolkit for Peacekeeping Operations.

UNCLASSIFIED information:

- ✓ Destroy official copies in accordance with the PORS.
- ✓ Use appropriate destruction methods.
- ✓ Avoid putting in trash bins, where possible.

12. DOWNGRADING

Downgrading is the process of reducing the classification level of information from the original classification level assigned to a lower classification level. Information can be downgraded based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. An example would be a STRICTLY CONFIDENTIAL record that would be reduced to a CONFIDENTIAL record after the passage of a specific time or event.

Whenever possible, the date or event that would trigger the downgrading of the information should be annotated on the document at the same time as the original classification level. Both the trigger date or event and the new security classification that will take effect upon the date or event should be annotated. The determination of a downgrade event or date during the original classification process ensures that the information will maintain the sensitivity level and protection required, and that the transition between classification levels will be seamless.

For example, a note relating to the SRSG's upcoming travel could simultaneously be marked as STRICTLY CONFIDENTIAL and be identified for downgrading to UNCLASSIFIED upon his or her return to mission headquarters.

STRICTLY CONFIDENTIAL
Downgrade to UNCLASSIFIED after completion of trip

Immediate

Note to Mr./Ms. Surname

SRSG Travel

Determine downgrade trigger events or dates during the original classification process.

Only the original classification authority, his or her successor, or a higher authority can downgrade information. If a request is received to downgrade a record prior to the downgrade trigger or for information that does not have a downgrade trigger, consult the office of origin or the office of origin's original classification authority to verify if the information may be downgraded.

Information with a security classification received from an external source cannot be downgraded without the external source's written approval. If a request to downgrade information classified by an external source is received, consult a staff member with original classification authority.

If a record is downgraded, and this downgrading action was not identified during the original classification process, the record must be marked with the new classification level and date it took effect. Additionally, all known holders of the information shall be notified of the new classification level assigned. Use the Sensitive Records Register to identify those individuals provided with the record.

13. DECLASSIFICATION

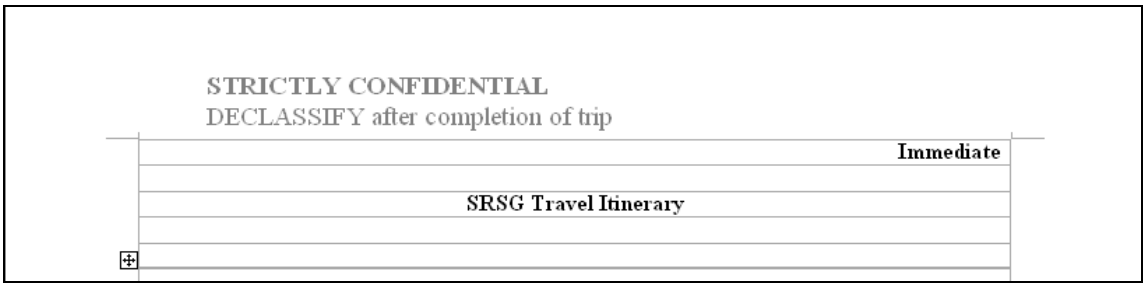
Declassification is the process of making previously classified material available for public consultation. Information can be declassified based on the loss of sensitivity of the information due to the passage of time, on occurrence of a specific event, or on the identification of a need to share the information with the general public.

Declassification normally is accomplished after the record or information is transmitted to the Archives and Records Management Section (ARMS) at UNHQ. However, there may be certain instances where records may be declassified before their transfer. Declassification may involve records that were generated and retained by the United Nations or those received from external sources bearing external security classifications. No classified record should be released without approval of the office of origin unless it has already undergone declassification.

Information received from an external source that bears a security classification cannot be declassified without the external source's written approval. If a request to declassify information classified by an external source is received, consult a staff member with original classification authority.

Classified information from an external source cannot be declassified without the external source's written approval.

Whenever possible, the date or event that would trigger the declassification of the information should be annotated on the document at the same time as the original classification level. Both the trigger date or event and the new security classification that will take effect upon the date or event should be annotated. For example, an SRSG's travel itinerary could simultaneously be marked as STRICTLY CONFIDENTIAL and be marked for declassification immediately upon his or her return to mission headquarters.



Determination of the declassification event or date during the original classification process ensures that the information will maintain the sensitivity level and protection required and that the transition between classification levels will be as simple as possible.

14. ROLES AND RESPONSIBILITIES

Roles and responsibilities for information sensitivity and security are:

- Head of Mission:
  - Ensures that ST/SGB/2007/6 and this Information Sensitivity Toolkit are implemented.
  - Determines general policy regarding staff member access to sensitive information.
- Chiefs of Sections in Mission:
  - Ensure that ST/SGB/2007/6 and this Information Sensitivity Toolkit are implemented.
  - Establish standard distribution lists for sensitive information of a recurrent nature.
- Information Management Officer in the Mission:
  - Ensures that information security controls are incorporated into paper and electronic information systems throughout the mission.
  - Provides advice and training to all staff members on information sensitivity and security.
- CITS in the Mission:
  - Ensures that information systems incorporate the concepts of ST/SGB/2007/6 and ST/SGB/2004/15.
  - Supports the proper management of electronic information systems.
- Staff Members in the Mission:
  - Follow ST/SGB/2007/6.
  - Follow the requirements of this Information Sensitivity Toolkit.
  - Ensure sensitive information is classified and marked appropriately.
  - Ensure that sensitive information is handled and stored appropriately.
  - Protect sensitive information.
- Information and Communications Technology Division, Department of Field Support, at UNHQ:
  - Provides support to CITS.
- Archives and Records Management Section, Department of Management, at UNHQ:
  - Provides support to the Information Management Officer in the application of this Information Sensitivity Toolkit.
- Peacekeeping Information Management Unit, Department of Peacekeeping Operations, at UNHQ:
  - Provides support to the Information Management Officer in the application of this Information Sensitivity Toolkit.
- Office of Information and Communications Technology, at UNHQ:
  - Provides support and guidance to CITS and DFS/ICTD.
  - Issues policies and guidelines for the operation of ICT systems that store, process or transmit sensitive information.

15. CASE STUDIES

In order to apply the requirements for information sensitivity, classification and handling, case studies are provided. Please review the case study and determine how you would handle each situation described.

- Case Study 1 - Sensitive Information Left on Co-Worker's Unattended Desk
- Case Study 2 - Sensitive Code Cable Left on Photocopier
- Case Study 3 - Request to Copy and Transmit a Record Classified by an External Source

16. COMPENDIUM OF EXAMPLES

A sample listing of records and possible security classifications is provided as Annex 17. This listing is provided as guidance only and does not represent the only security classification for the record listed. Since the level of security classification is based on the degree of damage that could be expected from unauthorized disclosure (i.e., extremely grave damage or cause damage to the work of the United Nations), records must be classified based on the content of the information they contain.

17. REFERENCE DOCUMENTS

Records Management

- ST/SGB/2007/6: Information sensitivity, classification and handling
- ST/SGB/2007/5: Recordkeeping and the management of United Nations archives
- DPKO and DFS Policy Directive: Records management
- DPKO and DFS SOP: Access and declassification of archives and non-current records
- DPKO and DFS Policy: Peacekeeping and political operations retention schedule (PORS)
- DPKO and DFS Guideline: Use of the peacekeeping and political operations retention schedule
- DPKO and DFS Circular Cable 1310 (6 June 2008): Marking code cables for sensitivity and dissemination
- DFS Circular Cable 1207 (1 June 2009): Use and classification of code cables regarding cases of alleged misconduct

Information Technology

- ST/SGB/2004/15: Use of information and communication technology resources and data

Human Resources

- ST/SGB/2009/6: Staff regulations
- ST/SGB/2002/13: Status, basic rights and duties of United Nations staff members
- ST/SGB/2002/9: Regulations governing the status, basic rights and duties of officials other than Secretariat officials, and experts on mission
- ST/AI/371: Revised disciplinary measures and procedures

18. GLOSSARY

Access – The right, opportunity or means of finding, using or retrieving information. The granting of permission, usually on a case-by-case basis, to examine and study individual archives and records; to extract information from archives and records for general consultation.

Archives – Those records that are appraised as having historical value and are no longer required for current use.

Classification – The act or process by which information is determined to be sensitive or non-sensitive information.

Declassification – The process of making previously restricted materials available for public consultation.

Disclosure – The process of reviewing documentary material to determine what material or parts of material must be withheld from a requestor because of access restrictions, and the process of implementing those decisions to release, redact, withdraw, or withhold materials. This includes systematic review, mandatory review, Freedom of Information Act (FOIA) review, special access review, and review of records of concern.

Document – Recorded information or object which can be treated as a unit. (*Source: International Standard ISO/TR 15489-1, Clause 3.10*)

Downgrading – The process of reducing the classification level of information from the original classification level to a lower classification level.

Electronic recordkeeping system – An automated system used to manage the creation, use, maintenance and disposal of electronically created records for the purposes of providing evidence of business activities. These systems maintain appropriate contextual information (metadata) and links among records to support their value as evidence. ERMS is a subset of business information systems whose primary purpose is the capture and management of digital records.

Handling – Transmitting and safeguarding of sensitive and non-sensitive information and includes sensitivity marking, transfer, storage, reproduction and disposal.

Information – Any knowledge that can be communicated or any documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United Nations. “Control” means the authority of the department, office or mission that originates information, or its successor in function, to regulate access to the information.

Information security – Policies and procedures to ensure that sensitive information is protected and appropriately accessed.

Marking – The process of placing identifiers on records showing the level of sensitivity assigned.

Need to know – Determining when a prospective recipient has a requirement for access to, knowledge of or possession of sensitive information to perform tasks or services.

Need to share – The individual and collective obligation to make information available, discoverable and accessible for those entities that require the information to perform their official tasks and services.

Office of origin – The mission section or office that creates a record or originally receives a record from an external source.

Office of record – The office or administrative unit that has been designated for the maintenance, preservation and disposition of record (official) copies.

Original classification – An initial determination that information requires, in the interest of organizational security, protection against unauthorized disclosure.

Original classification authority – An individual authorized in writing, either by the Head of Mission, or by section chiefs or other officials designated by the Head of Mission, to classify information in the first instance.

Original classification authority list – A list of staff members with original classification authority.

Public information – Information that is produced expressly for public consumption or that has undergone a declassification process and is now available for public disclosure.

Record(s) – The International Organization for Standardization (ISO) defines records as “information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business”. The International Council on Archives (ICA) Committee on Electronic Records defines a record as “recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity”.

Right to know – Implicitly sanctioned requirements for access to records in specific situations and under certain circumstances.

Security classification – A security level (STRICTLY CONFIDENTIAL, CONFIDENTIAL or UNCLASSIFIED) that is applied to records and which corresponds to the degree of sensitivity of information contained in those records.

Security violation – An event which could have led to unauthorized disclosure, but did not. Examples of security violations include alteration or retention of sensitive information without authorization or a failure to protect sensitive information.

Sensitive records register – A list, either paper or electronic, which identifies sensitive records received or copied including any event or date that would automatically trigger downgrading or declassification.

Sensitive information – Information that, as determined by the United Nations, must be protected because its unauthorized disclosure, alteration, loss or destruction will at least cause perceivable damage to the Organization, including its staff members, operations, security or international relations. In accordance with ST/SGB/2007/6, all sensitive information created or received by the United Nations in the course of its business must be marked as STRICTLY CONFIDENTIAL or CONFIDENTIAL.

Unauthorized disclosure – A communication or physical transfer of sensitive information to an unauthorized recipient.

Upgrading – The process of increasing the classification level of information from the original classification level to a higher classification level.

19. FREQUENTLY ASKED QUESTIONS (FAQS)

1. **Do I need to follow the requirements on information sensitivity if I am in a field mission?**
2. **How do I determine the level of classification between STRICTLY CONFIDENTIAL and CONFIDENTIAL information?**
3. **When should documents be classified?**
4. **Do the United Nations classification levels apply to information from external sources?**
5. **Are all code cables considered sensitive?**
6. **Is there a relationship between security classifications and the precedence indicators ‘Routine’, ‘Immediate’ and ‘Most Immediate’?**
7. **Do I need to follow all the steps for classifying information?**
8. **Do I need to include a trigger date or event for downgrading or declassification when I classify information?**
9. **How do I mark electronic records?**
10. **Does ‘need to know’ only apply to sensitive information?**
11. **What is meant by ‘right to know’?**
12. **What are the implications if information is released to unauthorized individuals?**
13. **Who is responsible to ensure sensitive information is handled correctly?**

14. **Who determines if an electronic system or application is safe to store sensitive information?**
15. **Who determines whether or not a sensitive document can be duplicated?**
16. **Can I send sensitive information via email?**
17. **Are the requirements for handling STRICTLY CONFIDENTIAL and CONFIDENTIAL information the same?**
18. **Are there any handling requirements for UNCLASSIFIED information?**
19. **What is meant by 'downgrading'?**
20. **Is declassification of records automatic?**
21. **What is the difference between classification and marking?**
22. **Is it OK to email a code cable?**
23. **How can I check my password strength?**
24. **How does one classify personal information?**

1. Do I need to follow the requirements on information sensitivity if I am in a field mission?

Yes. The requirements for handling and managing sensitive information apply to all staff members, seconded personnel, military contingents, and formed police units, regardless of their location. The challenge with proper management of sensitive information is magnified within peacekeeping operations due to the varied nature of the missions and the exceptional circumstances in which they operate.

2. How do I determine the level of classification between STRICTLY CONFIDENTIAL and CONFIDENTIAL information?

The appropriate classification level is determined by the disclosure risks of the information, which is usually determined by the magnitude, amount or kind of damage that could be caused by the unauthorized disclosure of the information. STRICTLY CONFIDENTIAL is applied when the disclosure could cause exceptionally grave damage or impede the conduct of the work of the United Nations; such damage is irreparable. CONFIDENTIAL is applied when the disclosure could cause damage, albeit reparable.

3. When should documents be classified?

Internally-drafted documents should be classified as soon as the information contained therein is determined to be sensitive. Sensitive records received from third parties should be classified immediately upon receipt. ALL sensitive records must be classified with United Nations and/or external markings before transmission or storage.

4. Do the United Nations classification levels apply to information from external sources?

Yes. You should apply the United Nations classification level that provides the same or greater level of protection as the classification assigned by the external source.

5. Are all code cables considered sensitive?

No. Code cables, like other business records, are deemed to be sensitive or not based on their contents, not on the means of transmission. Accordingly, code cables may be of any sensitivity level and thus may bear any one of the three United Nations security classifications. Note that for code cables, the marking CONFIDENTIAL must always be used in conjunction with the dissemination label ONLY, and the marking STRICTLY CONFIDENTIAL must always be used in conjunction with the dissemination label NO DISTRIBUTION. This policy was formally established in the peacekeeping group with the issuance of Circular Cable 1310 of 6 June 2008 on "Marking code cables for sensitivity and dissemination".

6. Is there a relationship between security classifications and the precedence indicators 'Routine', 'Immediate' and 'Most Immediate'?

No. The inclusion of a precedence indicator on a record simply advises the recipient on the relevant processing order of that record (i.e., whether to process it faster than other records or to process it as normal). Any precedence indicator may be used with any security classification.

7. Do I need to follow all the steps for classifying information?

Yes. The steps (in Section 7 of this toolkit) are required to ensure that information is classified at the correct level. As you classify information, you will notice which records are recurrent and, therefore, are assigned the same classification level.

8. Do I need to include a trigger date or event for downgrading or declassification when I classify information?

Whenever possible, the date or event that would trigger the downgrading or declassification of information should be annotated on the document at the same time as the original classification level. Identifying and marking the trigger date during the original classification process ensures that the information will maintain the sensitivity level and protection required and that the transition between classification levels will be as simple as possible.

9. How do I mark electronic records?

Due to the differences in electronic systems, strategies vary and prudent judgment must be exercised. Contact your mission's Communications and Information Technology Section for assistance.

10. Does 'need to know' only apply to sensitive information?

'Need to know' applies *primarily* to sensitive information; however, it may be appropriate to apply to certain non-sensitive information as well.

11. What is meant by 'right to know'?

'Right to know' refers to an individual staff member's ability to have access to records about themselves or to perform their job requirements. 'Right to know' often is sanctioned through approved Organizational policies and applies to specific situations.

12. What are the implications if information is released to unauthorized individuals?

Besides the possibility of damage to or impediment of work of the United Nations or its Member States or endangering the welfare and safety of individuals, unauthorized disclosure of sensitive information to third parties is identified as misconduct and can result in disciplinary actions against the staff member, seconded personnel, or member of a military contingent or formed police unit.

13. Who is responsible to ensure sensitive information is handled correctly?

It is the responsibility of each staff member to ensure that sensitive information is handled according to all the rules associated with the classification level.

14. Who determines if an electronic system or application is safe to store sensitive information?

Any electronic system or application that will be used with sensitive information or used for the storage, processing or transmission of sensitive information is required to be reviewed and deemed secure by the mission CITS, in consultation with OICT, the mission's Information Management Officer, Information and

Communications Technology Division (ICTD), DFS, and the Archives and Records Management Section (ARMS), DM, at United Nations Headquarters.

15. Who determines whether or not a sensitive document can be duplicated?

Sensitive materials may be duplicated only with the authorization of either the originator or the head of the receiving or originating section or office. This approval is implicit when duplication is performed in accordance with distribution lists for materials of a recurring nature.

16. Can I send sensitive information via email?

Generally, sensitive information should not be transmitted by email but should be transmitted as a code cable or hand delivered. However, if there is an emergency situation requiring transmission via email, the email must be encrypted. The Section Chief (or higher) should determine when email should be used for transmitting sensitive information.

17. Are the requirements for handling STRICTLY CONFIDENTIAL and CONFIDENTIAL information the same?

No. STRICTLY CONFIDENTIAL information has slightly stricter requirements due to the extremely grave damage that could occur should the information be disclosed to an unauthorized individual. That said, a greater distinction between the two may be found in associated access rules established by each mission: access rules for STRICTLY CONFIDENTIAL information generally are much more restrictive than those for CONFIDENTIAL information.

18. Are there any handling requirements for UNCLASSIFIED information?

Yes. Although UNCLASSIFIED records are not considered sensitive, they should be protected from unauthorized disclosure outside the United Nations. To this effect, there are specific handling requirements to ensure their protection.

19. What is meant by 'downgrading'?

Downgrading is the process of reducing the classification level of information from the original classification level to a lower classification level. An example would be a STRICTLY CONFIDENTIAL record that would be reduced to a CONFIDENTIAL record after the passage of a specific time or event.

20. Is declassification of records automatic?

It depends on the security classification. Information may be eligible for declassification after a specific date or event. If there is no declassification trigger (date or event) clearly marked on the record, UNCLASSIFIED and CONFIDENTIAL information will be declassified automatically after 20 years. STRICTLY CONFIDENTIAL information is NEVER automatically declassified, and requires a review of each record prior to declassification. Note that business records are destroyed in accordance with United Nations records retention rules, and with the exception of select materials, this destruction occurs well before the 20 year mark.

21. What is the difference between classification and marking?

'Classification' is the act or process by which information is determined to be sensitive or non-sensitive. It is an *assessment* of the information at hand. 'Marking' is the subsequent action of placing either physical or electronic identifiers on information (or its metadata) so that the security classification is readily apparent to users and recordkeeping systems, thereby facilitating proper access controls.

22. Is it OK to email a code cable?

Code cables should be treated just like all other records. UNCLASSIFIED code cables may be emailed as an attachment. However, ONLY/CONFIDENTIAL and NO DISTRIBUTION/STRICTLY CONFIDENTIAL code cables must not be emailed under any circumstances. Section 10d on Transmission of Sensitive Information describes the conditions under which selected information contained in sensitive code cables may be transmitted by email.

23. How can I check my password strength?

United Nations Secretariat staff can use the ICTD Password Strength Checker at http://ictd.dfs.un.org/security/pages/TestPwd/index.html.

24. How does one classify personal information?

United Nations staff members regularly handle personal information of staff members and others. This information ranges from the seemingly mundane (telephone numbers, home addresses, time and attendance details, index numbers) to the sensitive (performance appraisals, claims records, financial histories) and highly sensitive (medical histories, disciplinary records). Nevertheless, wherever personal information is explicitly linked to staff member names or other data which would render the staff member identifiable, the information must be classified as STRICTLY CONFIDENTIAL and handled accordingly. The classification STRICTLY CONFIDENTIAL is necessary to ensure that the information is not automatically declassified once 20 years old, which is the rule for CONFIDENTIAL and UNCLASSIFIED information.

MAIN THINGS TO REMEMBER ABOUT MANAGING SENSITIVE INFORMATION

- Records can contain sensitive information

- There are different degrees of sensitivity indicated by the three official United Nations Security Classifications; in descending order of sensitivity the classifications are: STRICTLY CONFIDENTIAL, CONFIDENTIAL and UNCLASSIFIED

- A classification of STRICTLY CONFIDENTIAL or CONFIDENTIAL *must* be applied to all records containing sensitive information

- A classification of UNCLASSIFIED *should* be applied to records that contain no sensitive information yet are internal to the Organization

- All staff have a responsibility to mark, handle and protect sensitive and internal information in accordance with guidelines

ANNEX 2

Table: United Nations Security Classifications: At a Glance			
Security Classification	**Definition**	**Examples**	**Declassification**
STRICTLY CONFIDENTIAL	The designation that shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause EXCEPTIONALLY GRAVE DAMAGE to or IMPEDE THE CONDUCT OF THE WORK of the United Nations.	• Secretary-General's travel records • Conduct and discipline report containing personally identifiable details	• As determined by originator • Never automatically declassified
CONFIDENTIAL	The designation that shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause DAMAGE TO THE WORK of the United Nations.	• Record relating to a contractor or vendor • Minutes of a meeting relating to a political matter	• As determined by originator • Automatic at 20 years
UNCLASSIFIED	The designation that shall apply to information or material whose unauthorized disclosure could reasonably be expected NOT TO CAUSE DAMAGE to the work of the United Nations.	• Records relating to an upcoming conference • Results-Based Budgets	• As determined by originator • Automatic at 20 years
PUBLIC*	Information produced expressly for public consumption or that has undergone a declassification process and is now available for public use.	• Security Council Resolutions • SRSG press statements	• None required • Already declassified

***Not an official United Nations Security Classification**

ANNEX 3

SAMPLE: ORIGINAL CLASSIFICATION AUTHORITY LIST*

STRICTLY CONFIDENTIAL Information**

- SRSG/Head of Mission
- Officials designated by the Head of Mission:
  - Deputy SRSG for Operations and Rule of Law
  - Deputy SRSG for Humanitarian Coordination and Rehabilitation, Recovery and Reconstruction
  - Force Commander
  - Director or Chief of Mission Support
  - Chief of Staff
  - Chief, Safety and Security Section
- Mission staff members delegated this classification authority

CONFIDENTIAL Information

- Officials with original STRICTLY CONFIDENTIAL classification authority
- Officials designated by the Head of Mission in the Sensitive Records Register - typically chiefs of:
  - Administrative Services
  - Civil Affairs
  - Human Rights
  - Integrated Support Services
  - Joint Military Committee Office
  - Joint Mission Analysis Centre
  - Joint Operations Centre
  - Legal Affairs
  - Office of the Spokesperson for the Head of Mission
  - Police
  - Political Affairs
- Mission staff members delegated this classification authority

Delegations of original classification authority:

- Shall be limited to the minimum required to perform the work of the section or office.
- Chiefs of services and sections are responsible for ensuring that designated subordinate officials have a demonstrated and continuing need to exercise the classification authority.
- Each delegation of original classification authority shall be in writing and submitted to the Office of the Head of Mission.
- Each delegation shall identify the official by name or position title.

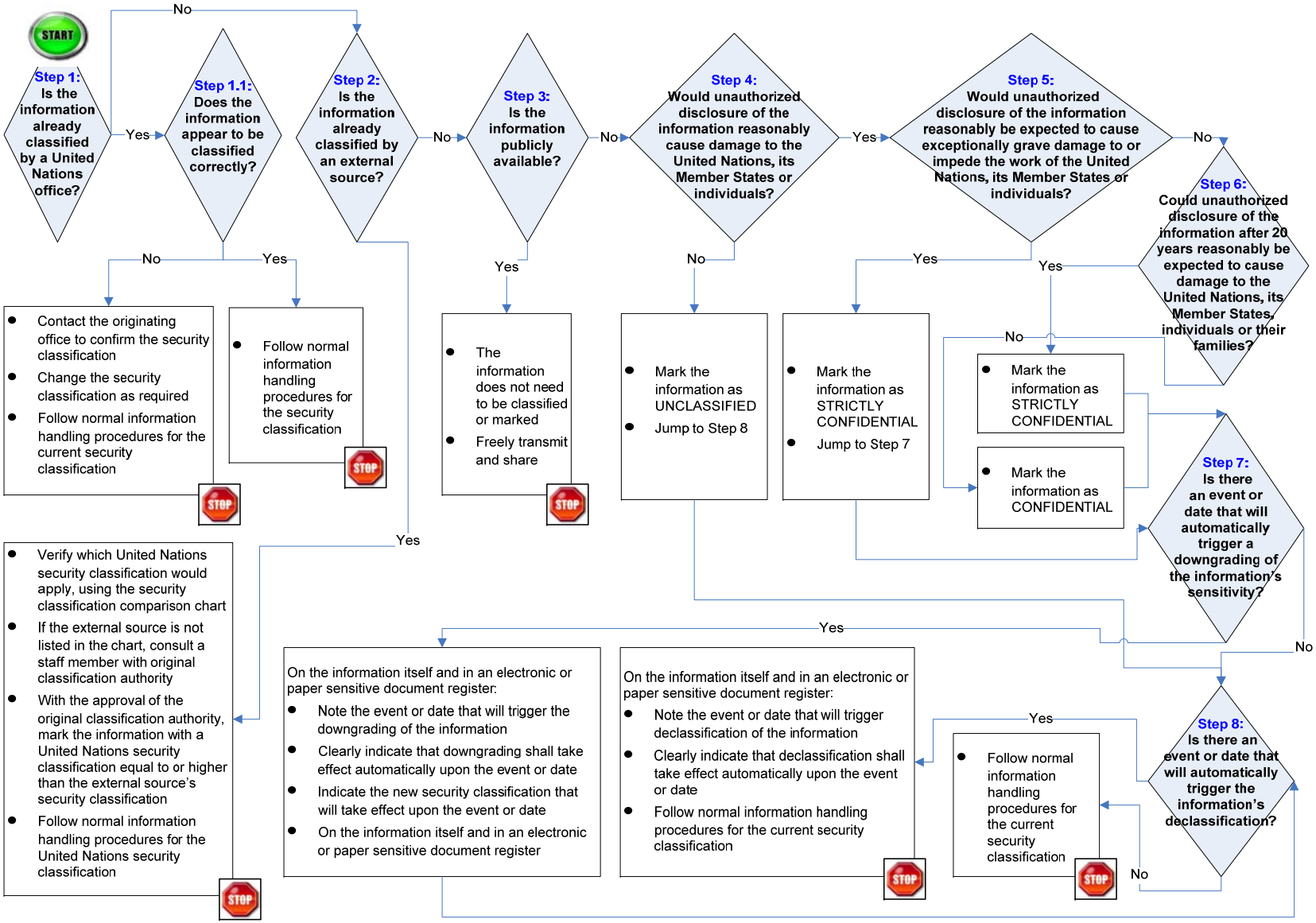
*For example purposes only; each mission should define its own original classification authority list, under the overall authority of the Head of Mission.

**** Note: all routine, personal information explicitly linked to staff member names or other data which would render the staff member identifiable (personal history profiles, time and attendance reports, medical leave certificates, etc.) are to be classified and marked as STRICTLY CONFIDENTIAL and handled accordingly. Therefore, all staff members handling personal information should exceptionally be granted STRICTLY CONFIDENTIAL original classification authority for this specific type of material.

ANNEX 4

Table: Comparison Chart for Classifying Externally Classified Records			
UNITED NATIONS Classification / OUTSIDE ENTITY	**UNCLASSIFIED**	**CONFIDENTIAL**	**STRICTLY CONFIDENTIAL**
European Union (EU)	Unclassified	Confidential; Confidential UE; Secret UE; Restreint UE	EU Top Secret; Très Secret UE
North Atlantic Treaty Organization (NATO)	NATO Unclassified (NU)	NATO Restricted (NR); NATO Confidential (NC)	NATO Secret (NS); Cosmic Top Secret (CTS)
United States, Federal Gov.	Unclassified	Confidential	Secret; Top Secret
Canada, Federal Gov.	Unclassified or designated as 'Protected A'	Confidential or designated as 'Protected B'	Secret, Top Secret or designated as 'Protected C'
France, Dept. of Defence	Non classifié	Confidentiel défense	Secret défense; Très secret défense
Australia **a) Dept. of Defence** **b) Federal Gov.**	a) Unclassified b) Unclassified	a) Restricted or Confidential b) 'X-in-confidence' or Protected	a) Secret or Top Secret b) Highly Protected
International Criminal Court (ICC)	*Administrative:* Public *Judicial:* Public	*Administrative:* Restricted & Confidential *Judicial:* Confidential	*Administrative:* Secret *Judicial:* Under Seal
Organisation for the Prohibition of Chemical Weapons (OPCW)	Yellow: Unclassified	Blue: Restricted Purple: Protected	Red: Highly Protected
Africa Union (AU)	Unclassified	Confidential	
	NIL or LOW SENSITIVITY	***MEDIUM SENSITIVITY***	***HIGH SENSITIVITY***

Disclaimer: The above listed security classifications do not reflect any official position or formal agreements between the United Nations and the respective third parties. They are indicated for reference purposes only.



ANNEX 5 – Classifying Information: The Main Steps

ANNEX 6

CLASSIFICATION CHECKLIST

☐ Is the record already classified by a United Nations office? If so, does it appear to be classified correctly?

☐ Was it classified by an external source? If so, what is the equivalent United Nations security classification for the external classification?

☐ Is it public information (information already in the public domain or which has undergone declassification)?

☐ Would unauthorized disclosure be expected to cause damage to the United Nations, its Member States or individuals?

☐ Would unauthorized disclosure be expected to cause exceptionally grave damage to the United Nations, its Member States or individuals, or to impede the work of the United Nations?

☐ Could unauthorized disclosure in 20 years still potentially cause damage?

☐ Is there a downgrading date or event?

☐ Is there a declassification date or event or would standard United Nations declassification rules apply?

☐ If the record could be considered STRICTLY CONFIDENTIAL or CONFIDENTIAL, do you have original classification authority to mark the record as such?

☐ If you do not have the authority, have you consulted someone in your office that does?

☐ Have you physically or electronically marked the record correctly?

ANNEX 7

ESTABLISHING BASELINE CRITERIA FOR AN ACCESS RIGHTS MATRIX

Below are the steps for establishing baseline access criteria and example of how an Office of the Director of Mission Support could follow the three steps and record the resulting information in an 'access rights matrix'. The office would then use this matrix to inform its 'need to know' decisions.

Step 1: Identify the types of business information for which your office is responsible

One way to quickly identify a mission office's core business records is to consult the Peacekeeping and Political Operations Retention Schedule (PORS), which lists the majority of mission records and arranges them by business activity. These clusters of records are called 'record series'. Each 'record series' has one or more designated 'offices of record', which are the offices who have primary responsibility for the maintenance, preservation and disposition of the corresponding record series.

The PORS lists a number of record series for which the Office of the Director of Mission Support holds primary responsibility. Three of these record series are:

Access Rights Matrix – Office of the Director of Mission Support					
Schedule	**Series Name**	**Notes**	**Office of Record**	**Access Rights**	**Restrictions**
PKO.PRO007	Procurement and Contracts Management: Contracting: advice: Local Committee on Contracts	Records include: Local Committee on Contracts meeting minutes and presentations	Office of the DMS		
PKO.PRP012	Property Management: Property survey: processing of accepted write-off requests	Records include: property survey AW case records	Office of the DMS		
PKO.SAF001	Safety Management: Policy, procedure, best practice	Records include: locally-produced policy and procedure relating to safety activities	Office of the DMS		

Step 2: Identify the types of staff members who require access

In certain instances, access rights may be readily apparent based on an individual's title, level or administrative support role. Examples include:

- Deputy Force Commander accessing sensitive military operations files.
- Human Resources Officer accessing staff member personnel files.

- Conduct and Discipline Officer accessing conduct case files.
- Human Rights Officer accessing human rights violation files.
- Personal Assistant to the SRSG seeing certain information required by or of the SRSG.

For the purposes of the Office of the Director of Mission Support, access rights could possibly be:

Access Rights Matrix – Office of the Director of Mission Support					
Schedule	**Series Name**	**Notes**	**Office of Record**	**Access Rights**	**Restrictions**
PKO.PRO007	Procurement and Contracts Management: Contracting: advice: Local Committee on Contracts	Records include: Local Committee on Contracts meeting minutes and presentations	Office of the DMS	• O/DMS staff members • Procurement Section staff • Resident Auditor	
PKO.PRP012	Property Management: Property survey: processing of accepted write-off requests	Records include: property survey AW case records	Office of the DMS	• O/DMS staff members • Office of the Chief, ISS • Resident Auditor	
PKO.SAF001	Safety Management: Policy, procedure, best practice	Records include: locally-produced policy and procedure relating to safety activities	Office of the DMS	• All mission staff (Need to share)	

- ✓ Although the Office of Record may have overall responsibility for the management of the record series, it may or may not be the Office of Origin.
- ✓ An Office of Origin is the mission office that creates a record or originally receives a record from an external source.
- ✓ In cases where the Office of Record and Office of Origin are different, the former will need to consult the latter in access rights decisions.

Step 3: Identify any restrictions to this information based on security classification or other parameters

In certain cases, information identified as STRICTLY CONFIDENTIAL or CONFIDENTIAL may be restricted to a certain sub-set of the groups identified in the 'Access Rights' column. Restrictions based on

other factors (e.g. record or document type) may also be taken into consideration. Wherever a senior staff member is identified, access rights by his or her personal assistant are inherent.

Access Rights Matrix – Office of the Director of Mission Support					
Schedule	**Series Name**	**Notes**	**Office of Record**	**Access Rights**	**Restrictions**
PKO.PRO007	Procurement and Contracts Management: Contracting: advice: Local Committee on Contracts	Records include: Local Committee on Contracts meeting minutes and presentations	Office of the DMS	• O/DMS staff members • Procurement Section staff • Resident Auditor	STRICTLY CONFIDENTIAL: P4 staff and above
PKO.PRP012	Property Management: Property survey: processing of accepted write-off requests	Records include: property survey AW case records	Office of the DMS	• O/DMS staff members • Office of the Chief, ISS • Resident Auditor	STRICTLY CONFIDENTIAL: • DMS • Chief, ISS • Resident Auditor
PKO.SAF001	Safety Management: Policy, procedure, best practice	Records include: locally-produced policy and procedure relating to safety activities	Office of the DMS	• All mission staff (Need to share)	CONFIDENTIAL: P4 and above STRICTLY CONFIDENTIAL: D1 and above

- ✓ 'Need to know' is determined on a record-by-record basis.
- ✓ Inclusion in any access rights matrices, such as the one above, does not imply that an identified staff member or group has full access rights to a particular record series.
- ✓ The Office of Origin reserves the right to restrict access to information should the requestor not have a clear 'need to know'.

ANNEX 8

TEMPLATE: ACCESS RIGHTS MATRIX

Office:
Date last updated:

Schedule*	Series Name*	Notes*	Office of Record*	Access Rights**	Restrictions***

*Refer to the Peacekeeping and Political Operations Retention Schedule (PORS).
**List here groups or individuals who generally require access to the information to perform their duties.
***Record here any restrictions on access based on security classification or other parameter.

ANNEX 9

TEMPLATE: SENSITIVE RECORDS REGISTER

Document Type	Sender or Originator	Document Date	Reference No.	Title (or Subject)	Total No. Received or Produced	Copy No.	Sec. Class.	Transmitted to (address, details)	Date Transmitted	Date Receipt Returned	Remarks

This information may be recorded in a standard Microsoft Excel or Word table or incorporated into the metadata set for your mission's electronic recordkeeping system.

ANNEX 10

Template: Code Cable Distribution List (add or remove rows as required)

Cable Security Classification / Cable Topic	Unclassified						Confidential					Strictly Confidential		
Budget														
Civil Affairs														
Disarmament, Demobilization, Reintegration														
Elections														
Facilities & Engineering														
Finance														
Governance														
Human Resources														
Human Rights														
Humanitarian Affairs														
Information Management														
Judicial & Legal Systems														
Law Enforcement														
Legal														
Management & Integration														
Military														
Mine Action														
Movement & Transport														
Oversight														
Political Affairs														
Prisons & Corrections Services														
Procurement & Contracts Management														
Property Management														
Public Information & Communications														
Safety Management														
Security Management														
Security Sector Reform														
Translation & Interpretation														

Acronyms (add to the above table as appropriate)

[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]
[Office Name]	[Acronym]	[Office Name]	[Acronym]

ANNEX 11

Sample: Code Cable Distribution List (For Example Purposes Only)															
Cable Security Classification / Cable Topic (FCS* Category)	Unclassified						Confidential					Strictly Confidential		
Budget	OSRSG	JOC	OCOS	DOA	AS		OSRSG	JOC	OCOS	DOA		OSRSG	JOC	
Civil Affairs	OSRSG	JOC	OCOS	ODSRSG-O	CAS		OSRSG	JOC	OCOS	ODSRSG-O	CAS	OSRSG	JOC	ODSRSG-O
Disarmament, Demobilization, Reintegration	OSRSG	JOC	OCOS	ODSRSG-O	RRRS		OSRSG	JOC	OCOS	ODSRSG-O	RRRS	OSRSG	JOC	ODSRSG-O
Elections	OSRSG	JOC	OCOS	ODSRSG-O	ED		OSRSG	JOC	OCOS	ODSRSG-O	ED	OSRSG	JOC	ODSRSG-O
Facilities & Engineering	OSRSG	JOC	OCOS	DOA	ISS		OSRSG	JOC	OCOS	DOA		OSRSG	JOC	
Finance	OSRSG	JOC	OCOS	DOA	AS		OSRSG	JOC	OCOS	DOA		OSRSG	JOC	
Governance	OSRSG	JOC	OCOS				OSRSG	JOC	OCOS			OSRSG	JOC	
Human Resources	OSRSG	JOC	OCOS	DOA	AS		OSRSG	JOC	OCOS	DOA		OSRSG	JOC	
Human Resources: Administration of Justice**	OSRSG	JOC	OCOS				OSRSG	JOC	OCOS			OSRSG	OCOS	
Human Rights	OSRSG	JOC	OCOS	ODSRSG-O	HRPS		OSRSG	JOC	OCOS	ODSRSG-O	HRPS	OSRSG	JOC	ODSRSG-O
Humanitarian Affairs	OSRSG	JOC	OCOS	ODSRSG-H	HCS	RRRS	OSRSG	JOC	OCOS	ODSRSG-H	HCS	OSRSG	JOC	ODSRSG-H
Information Management	OSRSG	JOC	OCOS	DOA	ISS		OSRSG	JOC	OCOS	DOA		OSRSG	JOC	
Judicial & Legal Systems	OSRSG	JOC	OCOS	ODSRSG-O	LJSSD		OSRSG	JOC	OCOS	ODSRSG-O	LJSSD	OSRSG	JOC	ODSRSG-O
Law Enforcement	OSRSG	JOC	OCOS	ODSRSG-O	PC		OSRSG	JOC	OCOS	ODSRSG-O	PC	OSRSG	JOC	ODSRSG-O
Legal	OSRSG	JOC	OCOS				OSRSG	JOC	OCOS			OSRSG	JOC	
Management & Integration	OSRSG	JOC	OCOS	DOA			OSRSG	JOC	OCOS	DOA		OSRSG	JOC	OCOS
Military	OSRSG	JOC	OCOS	MC			OSRSG	JOC	OCOS	MC		OSRSG	JOC	MC
Mine Action	OSRSG	JOC	OCOS				OSRSG	JOC	OCOS			OSRSG	JOC	
Movement & Transport	OSRSG	JOC	OCOS	DOA	ISS		OSRSG	JOC	OCOS	DOA		OSRSG	JOC	
Oversight	OSRSG	JOC	OCOS	DOA			OSRSG	JOC	OCOS	DOA		OSRSG	JOC	DOA
Political Affairs	OSRSG	JOC	OCOS	ODSRSG-O			OSRSG	JOC	OCOS	ODSRSG-O		OSRSG	JOC	ODSRSG-O
Prisons & Corrections Services	OSRSG	JOC	OCOS	ODSRSG-O	CPAS		OSRSG	JOC	OCOS	ODSRSG-O	CPAS	OSRSG	JOC	ODSRSG-O
Procurement & Contracts Management	OSRSG	JOC	OCOS	DOA	ISS		OSRSG	JOC	OCOS	DOA	ISS	OSRSG	JOC	
Property Management	OSRSG	JOC	OCOS	DOA	ISS		OSRSG	JOC	OCOS	DOA		OSRSG	JOC	
Public Information & Communications	OSRSG	JOC	OCOS				OSRSG	JOC	OCOS			OSRSG	JOC	
Safety Management	OSRSG	JOC	OCOS	DOA			OSRSG	JOC	OCOS	DOA		OSRSG	JOC	
Security Management	OSRSG	JOC	OCOS				OSRSG	JOC	OCOS			OSRSG	JOC	
Security Sector Reform	OSRSG	JOC	OCOS	ODSRSG-O	LJSSD		OSRSG	JOC	OCOS	ODSRSG-O	LJSSD	OSRSG	JOC	ODSRSG-O
Translation & Interpretation	OSRSG	JOC	OCOS	DOA			OSRSG	JOC	OCOS	DOA		OSRSG	JOC	

Acronyms (add to the above table as appropriate)

Office of the Special Representative of the Secretary-General	OSRSG	Office of the Deputy Special Representative of the Secretary-General (Humanitarian Coordination, Rehabilitation, Recovery & Reconstruction)	ODSRSG-H
Joint Operations Centre	JOC	Humanitarian Coordination Section	HCS
Joint Mission Analysis Centre	JMAC	Relief, Rehabilitation, and Recovery Section	RRRS
Office of the Chief of Staff (Civilian)	OCOS	Military Component	MC
Office of the Deputy Special Representative of the Secretary-General (Operations & Rule of Law)	ODSRSG-O	Division of Administration	DOA
Civil Affairs Section	CAS	Integrated Support Services	ISS
Corrections and Prison Advisory Service	CPAS	Administrative Services	AS
Electoral Division	ED		
Human Rights and Protection Section	HRPS		
Legal and Judicial System Support Division	LJSSD		
Police Component	PC		

***Peacekeeping File Classification Scheme**
****Includes all conduct and discipline matters**

ANNEX 12

Quick Guide Information Marked as STRICTLY CONFIDENTIAL (Page 1 of 3)	
Definition	The designation STRICTLY CONFIDENTIAL shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of the work the United Nations. (ST/SGB/2007/6 Section 2.3)
Access	• Consult originator or the original classification authority to verify individual is authorized to access the information. • Use need to know: o Only those individuals who must have access to carry out their jobs or other strong justification. o Determined by the staff member processing the information, in consultation with the office of origin. o Requires a clear delegation of authority from the originator or staff member who originally applied the classification level. o Only disclosed to trusted individuals.
Marking	The following classification shall be used: STRICTLY CONFIDENTIAL. <u>Marking Paper Records</u> • The classification is NOT abbreviated. • Is in all BOLD uppercase letters larger than the print of the record. • Must be marked with the highest classification level of information contained in the record. • Located at the top of EACH page including all internal pages, front covers or title pages and on the back of the last page of bound material. • Filing folders must also be marked in the same manner as paper records. <u>Marking Electronic Records</u> • Contact mission CITS for databases or other types of systems or applications holding STRICTLY CONFIDENTIAL information. Note that the term “No Distribution” is not a substitute for STRICTLY CONFIDENTIAL. A code cable marked as “No Distribution” must be additionally marked and handled as a STRICTLY CONFIDENTIAL record.

Quick Guide Information Marked as STRICTLY CONFIDENTIAL (Page 2 of 3)	
Physical Security	• Filed in locked containers that are in locked rooms in areas under United Nations control. • Keys to lockable containers and rooms must be accounted for and tracked, and issued to the absolute smallest number of staff members possible. • Safe combinations should be assigned to the absolute smallest number of staff members possible. • Safe combinations should be changed immediately upon any indication of compromise. • Must be kept under constant surveillance when removed from storage. • Must be protected from unauthorized view until returned to secured storage. • Office should be locked when staff member leaves even for lunch or break. • Destruction bins are to remain locked at all times. • Maintain a 'clean desk' policy where no STRICTLY CONFIDENTIAL information is left on desks when the authorized user steps away – even for a moment. • Remain cognizant of persons in office areas. • In the absence of an electronic recordkeeping system, a hard copy of STRICTLY CONFIDENTIAL information received in an electronic form must be printed when received and filed and stored.
Use of Information Systems	• Automated information systems must have controls that prevent access by unauthorized persons and ensure the integrity of the information. • Should be maintained only in electronic systems deemed secure by the mission CITS, in consultation with DFS/ICTD and OICT. • If information is moved or transferred from one system or application to another, the access level must be assured to remain at the same level. • User access to electronic systems of applications must be reviewed and access levels differentiated to ensure staff members have the correct level of access. • Access rights should be reviewed and changed or terminated when a user changes positions or offices.
Use of Desktop Computers	• Do not use the hard drive (C: drive) to store STRICTLY CONFIDENTIAL information. • Utilize secure network drives, preferably authorized user's (i.e. H:) drive (contact CITS if needed). • 'Clean up' computer and network locations by deleting unnecessary copies and old records which have met their retention periods. • Utilize the automatic time out/lock feature of computer.
Removable Electronic Media including Laptop Computers	• All removable electronic media and laptops should be encrypted. • When travelling, ensure only required information is stored on removable electronic media or laptop computers. • When travelling, hand-carry all removable electronic media and laptop computers. Do NOT put them into checked baggage. • Utilize the automatic time out/lock feature of the laptop computer.
Duplication	• Only with authorization of originator or the head of the receiving or originating section or office. • Where possible, maintain a single consultation copy of STRICTLY CONFIDENTIAL information, rather than creating one or more convenience copies. • Use photocopies and printers that are secured or attended. • If using unsecured machines, ensure you immediately go to the machine after completing the "send" or "print" command; if available, take advantage of the printer's or copier's PIN features. • Duplication activities must be recorded in a Sensitive Records Register.

Quick Guide Information Marked as STRICTLY CONFIDENTIAL (Page 3 of 3)	
Sender of Information	• Establish that there is a need to share or ensure the recipient of the information has an established need to know or right to know status. • Ensure transferred by the most secure means possible. • Ensure properly classified at the point of origin. • Ensure recipient understands handling requirements. • Ensure recipient supplies a receipt for the information.
Recipient of Information	• Acknowledge receipt of information. • Ensure originator has applied appropriate classification. • Contact originator if applied classification needs adjustment. • Never change classification without the originator's consent. • Document originator's consent alongside copy maintained in central file. • Ensure appropriate handling of the information.
Paper Record Transmission	• Use the United Nations pouch system. • Transport in double-sealed envelopes or containers, with only the internal envelope or container clearly marked with STRICTLY CONFIDENTIAL. • Use correct level of staff for hand delivery. • Send on a one-to-one basis (i.e., from one person to one person) where possible. • Recurrent STRICTLY CONFIDENTIAL information should be transmitted through established distribution lists. • Must not be disseminated outside the mission area without consent of the originating office or higher authority. • Must be transmitted separately from information with lower level classifications. • All transmittal of all outgoing and incoming STRICTLY CONFIDENTIAL information must be recorded in a Sensitive Records Register.
Email Transmission	• Should not be used to transmit STRICTLY CONFIDENTIAL information. • Section Chief (or higher) should determine when email should be used. • If used, email must be encrypted. • Verify each time before sending that the email is addressed to the correct person(s). • Verify on a regular basis that the email distribution lists are correct and up-to-date. • The sender and/or recipient may be required to print the email for filing and preservation. • Send email to as few recipients as possible. • Do not indicate classification level in the email itself.
Fax Transmission	• Must not be used to transmit STRICTLY CONFIDENTIAL information.
Destruction	• Destroy in accordance with the Peacekeeping and Political Operations Retention Schedule (PORS). • Use appropriate secure destruction method for the media and format. • Do not put in trash bins. • Should be placed in lockable containers while awaiting destruction. • Specific information on the destruction of STRICTLY CONFIDENTIAL information in different media and formats can be found in the Recordkeeping Toolkit for Peacekeeping Operations.

ANNEX 13

Quick Guide Information Marked as CONFIDENTIAL (Page 1 of 3)	
Definition	The designation CONFIDENTIAL shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause damage to the conduct of the work the United Nations. (ST/SGB/2007/6 Section 2.3)
Access	• Consult originator or the original classification authority to verify individual is authorized to access the information. • Use need to know: o Only those individuals who must have access to carry out their jobs or other strong justification. o Determined by the staff member processing the information, in consultation with the office of origin. o Requires a clear delegation of authority from the originator or staff member who originally applied the classification level. o Only disclosed to trusted individuals.
Marking	The following classification shall be used: CONFIDENTIAL. <u>Marking Paper Records</u> • The classification is NOT abbreviated. • Is in all BOLD uppercase letters the same font as the print of the record. • Must be marked with the highest classification level of information contained in the record. • Located at the top of EACH page including all internal pages, front covers or title pages and on the back of the last page of bound material. • Filing folders must also be marked in the same manner as paper records. <u>Marking Electronic Records</u> • Contact mission CITS for databases or other types of systems or applications holding CONFIDENTIAL information. Note that the term “Only” is not a substitute for CONFIDENTIAL. A code cable marked as “Only” must be additionally marked and handled as a CONFIDENTIAL record.

Quick Guide Information Marked as CONFIDENTIAL (Page 2 of 3)	
Physical Security	• Filed in locked containers or locked rooms in areas under United Nations control. • Keys to lockable equipment and rooms must be accounted for and tracked. • Safe combinations assigned only to appropriate staff. • Safe combinations should be changed immediately upon any indication of compromise. • Must be kept under constant surveillance when removed from storage. • Must be protected from unauthorized view until returned to secured storage. • Destruction bins are to remain locked at all times. • Maintain a 'clean desk' policy where no information is left on desk or in offices when staff member leaves for extended periods or at end of work shift. • Remain cognizant of persons in office areas. • In the absence of an electronic recordkeeping system, a hard copy of CONFIDENTIAL information received in an electronic form must be printed when received and filed and stored.
Use of Information Systems	• Automated information systems must have controls that prevent access by unauthorized persons and ensure the integrity of the information. • Should be maintained only in electronic systems deemed secure by the mission CITS, in consultation with DFS/ICTD and OICT. • If information is moved or transferred from one system or application to another, the access level must be assured to remain at the same level. • User access to electronic systems of applications must be reviewed and access levels differentiated to ensure staff members have the correct level of access. • Access rights should be reviewed and changed or terminated when a user changes positions or offices.
Use of Desktop Computers	• Do not use the hard drive (C: drive) to store CONFIDENTIAL information. • Utilize secure network drives, preferably authorized user's (i.e. H:) drive (contact CITS if needed). • 'Clean up' computer and network locations by deleting unnecessary copies and old records which have met their retention periods. • Utilize the automatic time out/lock feature of computer.
Removable Electronic Media including Laptop Computers	• All removable electronic media and laptops should be encrypted. • When travelling, ensure only required information is stored on removable electronic media or laptop computers. • When travelling, hand-carry all removable electronic media and laptop computers. Do NOT put them into checked baggage. • Utilize the automatic time out/lock feature of the laptop computer.
Duplication	• Only with authorization of originator or the head of the receiving or originating department or office. • Ensure only required copies are made and provided. • Use photocopies and printers that are secured or attended. • If using unsecured machines, ensure you immediately go to the machine after completing the "send" or "print" command; if available, take advantage of the printer's or copier's PIN features. • Duplication activities must be recorded in a Sensitive Records Register.

Quick Guide Information Marked as CONFIDENTIAL (Page 3 of 3)	
Sender of Information	• Establish that there is a need to share or ensure the recipient of the information has an established need to know or right to know status. • Ensure transferred by the most secure means possible. • Ensure properly classified at the point of origin. • Ensure recipient understands handling requirements. • Ensure recipient supplies a receipt for the information.
Recipient of Information	• Acknowledge receipt of information. • Ensure originator has applied appropriate classification. • Contact originator if applied classification needs adjustment. • Never change classification without the originator's consent. • Document originator's consent alongside copy maintained in central file. • Ensure appropriate handling of the information.
Paper Record Transmission	• Use the United Nations pouch system. • Transport in double-sealed envelopes or containers, with only the internal envelope or container clearly marked with CONFIDENTIAL. • Use correct level of staff for hand delivery. • Send on a one-to-one basis (i.e., from one person to one person) where possible. • Recurrent CONFIDENTIAL information should be transmitted through established distribution lists. • Mission information classified as CONFIDENTIAL may be disseminated within the Secretariat unless prohibited by the originator. • The transmittal of all outgoing and incoming CONFIDENTIAL information must be recorded in a Sensitive Records Register.
Email Transmission	• Should not be used to transmit CONFIDENTIAL information. • Section Chief (or higher) should determine when email should be used. • If used, email must be encrypted. • Verify each time before sending that the email is addressed to the correct person(s). • Verify on a regular basis that the email distribution lists are correct and up-to-date. • The sender and/or recipient may be required to print the email for filing and preservation. • Send the email to as few recipients as possible. • Do not indicate classification level in the email itself.
Fax Transmission	• Must not be used to transmit CONFIDENTIAL information.
Destruction	• Destroy in accordance with the Peacekeeping and Political Operations Retention Schedule (PORS). • Use appropriate secure destruction method for the media and format. • Do not put in trash bins. • Should be placed in lockable containers while awaiting destruction. • Specific information on the destruction of CONFIDENTIAL information in different media and formats can be found in the Recordkeeping Toolkit for Peacekeeping Operations.

ANNEX 14

INFORMATION SENSITIVITY TOOLKIT
CASE STUDY 1

Sensitive Information Left on Co-Worker's Unattended Desk

It is 6:00 p.m. and you notice that your colleague has left the office. The door to his office is open and there is a STRICTLY CONFIDENTIAL record visible on his desk. You notice this record from the doorway as you are preparing to leave for the evening. This is the first time that you have noticed this type of negligence from this co-worker. You are aware of the requirements to protect sensitive information and you also know that a cleaning service will be in the office later in the evening.

- **What would you do?**
- **What steps would you take?**
- **What type of follow up would you perform?**

INFORMATION SENSITIVITY TOOLKIT
CASE STUDY 1

Sensitive Information Left on Co-Worker's Unattended Desk

RESPONSE

There are several actions to take. Remember that this co-worker has NOT left sensitive information or records unsecured in the past.

- Your immediate action should be to secure the record so that the information is not disclosed.
- You should lock the record in your desk, a lockable cabinet or lockable room used for sensitive information.
- You should provide your colleague with a note on his desk notifying him that you have secured the record and where it is secured. (He may not have left for the day and may be returning to his office to work further with the document.)
- The next morning (or as soon as you see your co-worker) you should provide him with the record, if he has not already retrieved it.
- You should discuss with your co-worker your concern about the sensitive information being left unsecured at the end of the day and explain where the policy and procedures are located on handling sensitive information.
- If this is the first time and no damage was done, e.g., no one else obtained the information, securing the record and talking with your co-worker should be sufficient.

If this is NOT the first time that you have secured sensitive information left out by this co-worker and as far as you can tell no damage was incurred, you should take additional steps. Since talking with your co-worker after the previous incident did not appear to ensure that he did not leave sensitive information unsecured, escalated action should be employed to ensure that sensitive information is protected.

- Your immediate action should be to secure the record so that the information is not disclosed.
- You should lock the record in your desk, a lockable cabinet or lockable room used for sensitive information.
- You should provide your colleague with a note on his desk notifying him that you have secured the record and where it is secured. (He may not have left for the day and may be returning to his office to work further with the record.) In the note, you should state that since this is not the first time that this has happened, you have (or will) contact his supervisor of the violation in handling sensitive information.
- Either notify his supervisor that evening, if his supervisor is still on premises, or send his supervisor an email that you wish to speak with him or her first thing in the morning but do not provide incriminating details in the email about the situation. Use a generic statement that you wish to speak with him or her about the handling of sensitive information in the office.
- At the first opportunity, discuss the situation with the supervisor and allow him or her to handle it from that point.

Whether or not leaving the sensitive information was a first time occurrence, if it appears that damage was done (i.e., you have reason to believe that an unauthorized person has looked at, copied or otherwise used the information) you should:

- Notify mission security immediately.
- Follow mission security's instructions for your next actions.

At no time should you allow the sensitive information to be left unsecured. If you do nothing, you are also in violation of the procedures for handling sensitive information.

ANNEX 15

INFORMATION SENSITIVITY TOOLKIT
CASE STUDY 2

Sensitive Code Cable Left on Photocopier

All network printers and photocopiers of the mission are located in corridors or open office areas, accessible by all staff and contractors including builders, cleaners, etc. You notice that someone has left a “No Distribution/STRICTLY CONFIDENTIAL” code cable relating to a military matter on a copier next to the Office of the Force Commander.

- **What would you do?**
- **What steps do you take?**
- **What type of follow up would you perform?**

INFORMATION SENSITIVITY TOOLKIT
CASE STUDY 2

Sensitive Code Cable Left on Photocopier

RESPONSE

It would be best if printers and copiers that print or photocopy sensitive information are located in secured areas and only accessible to those with appropriate clearance and authority. In many instances, this is not the case.

The immediate steps you should take include:

- Immediately take the record from the copier to reduce the possibility of unauthorized disclosure.
- Based on the knowledge that the information in the code cable relates to a military matter, take the copy to the Personal Assistant to the Force Commander and explain where you found the copy. See if you or he or she can determine who would have left the copy unattended on the copier.
- If identified, inform the staff member who left the copy on the copier that you found the copy and when, so they can determine whether or not there could have been a breach or unauthorized disclosure.
- Discuss with your supervisor the problem of finding the STRICTLY CONFIDENTIAL record on the photocopier and the implications. Suggest if there may be a more secure location for the copier or whether it would be appropriate for “reminder” training on the procedures for using unsecured and unattended photocopiers for copying sensitive information.
- Remember, sensitive information should not be printed or copied on unsecured or unattended printers and photocopiers. When it is required to use an unsecured or unattended printer or photocopier, you should immediately go to the printer or photocopier once you have “sent” the record to the machine.

ANNEX 16

INFORMATION SENSITIVITY TOOLKIT
CASE STUDY 3

Request to Copy and Transmit a Record Classified by an External Source

You are the Personal Assistant to the SRSG. T he Special Assistant to the SRSG comes back from a meeting and hands over to you a European Union record classified "Restreint UE" and asks you to copy and transmit it.

- **What would you do?**
- **What steps would you take?**
- **What type of follow up would you perform?**

INFORMATION SENSITIVITY TOOLKIT
CASE STUDY 3

Request to Copy and Transmit a Record Classified by an External Source

RESPONSE

There are several steps that you should take when presented with this situation.

- Verify the equivalent United Nations security classification for European Union “Restreint UE”. (It is CONFIDENTIAL.) Remember that the procedures and handling of sensitive information extend to those records classified by an external source.
- Verify if the Special Assistant to the SRSG has original classification authority. If not, inform the Special Assistant to the SRSG that you must verify the transmission of the record with the appropriate staff member with classification authority for the information.
- Have the appropriate classification authority mark or verify the security classification for the information.
- Verify with the classification authority that the transmission requested by the Special Assistant to the SRSG is appropriate and the entire distribution list has a need to know for the information.
- If approval to copy and transmit is granted, copy and transmit using the established procedures to ensure the protection of the sensitive information.
- Record the information about the transmission and copy in the appropriate sensitive records register.

ANNEX 17

Records and Possible Security Classifications
For instructional purposes only - Not an exhaustive list

Example records	Possible Security Classification	Caveat*	Declassification Rule	Possible Downgrading Trigger	Possible Declassification Trigger	FCS** Code 1	FCS Code 2	FCS Function	FCS Activity
Accident investigation reports	Confidential	E	Automatic at 20 years	Originator determined	Originator determined	SEC	7	Security Management	Investigation
Analysis of an event	Confidential	C	Automatic at 20 years	When event has passed	Originator determined	MIL	4	Military	Monitoring, reporting
Ballot papers	Strictly Confidential	D	SG declassification decision	None	When election results are confirmed	ELE	10	Elections	Balloting
Blue prints of mission facilities	Strictly Confidential	C	SG declassification decision	Facility undergoes significant structural change	Mission closure	FEN	7	Facilities and Engineering	Facilities development
Boards of Inquiry reports	Strictly Confidential	B	SG declassification decision	None	None	OVE	11	Oversight	Inquiry
Border committee deliberation records	Confidential	A	Automatic at 20 years	Information superseded	Border dispute resolved	POL	10	Political Affairs	Support to demarcation efforts
Campaign records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	ELE	9	Elections	Nominations and campaigning
Claims Review Board meeting minutes	Strictly Confidential	B	SG declassification decision	None	None	FIN	7	Finance	Claims review
Comparative evaluation reports	Strictly Confidential	B	SG declassification decision	None	None	HRM	9	Human Resources	Appointment and assignment
Conference records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	POL	3	Political Affairs	Coordination, partnership
Congratulatory letters	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	PUC	10	Public Information and Communications	Protocol
Daily military monitoring reports	Confidential	C	Automatic at 20 years	48 hours	Originator determined	MIL	4	Military	Monitoring, reporting
Daily mission situation reports	Confidential	C	Automatic at 20 years	48 hours	Originator determined	MAT	4	Management and Integration	Monitoring, reporting
Damage discrepancy reports	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	PRP	11	Property Management	Receiving and inspection
Draft laws	Confidential	A	Automatic at 20 years	None	Law adopted	JDL	9	Judicial and Legal Systems	Legislative reform
Draft Secretary-General's report on a mission	Confidential	E	Automatic at 20 years	Approval by EOSG	Publication of report	MAT	4	Management and Integration	Monitoring, reporting
Electoral assessment report	Confidential	C	Automatic at 20 years	Originator determined	Election completed	ELE	1	Elections	Planning, strategy
Electoral register	Strictly Confidential	B	SG declassification decision	None	None	ELE	8	Elections	Registering voters
ePAS reports	Strictly Confidential	B	SG declassification decision	None	None	HRM	24	Human Resources	Performance appraisal, recognition
Evaluation sheets from preliminary interviews	Strictly Confidential	B	SG declassification decision	None	None	HRM	8	Human Resources	Recruitment and outreach
Examination test results	Strictly Confidential	B	SG declassification decision	None	None	HRM	7	Human Resources	Examination administration
Ex-combatant records	Strictly Confidential	B	SG declassification decision	None	None	DDR	9	Disarmament, Demobilization, Reintegration	Reintegration
External audit reports	Confidential	E	Automatic at 20 years	Originator determined	Originator determined	OVE	8	Oversight	External Audit
Facilities service requests	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	FEN	12	Facilities and Engineering	Facilities service provision
Fire investigation reports	Confidential	E	Automatic at 20 years	Originator determined	Originator determined	SAF	7	Safety Management	Investigation
Force Commander end of assignment report	Confidential	E	Automatic at 20 years	Originator determined	Originator determined	MAT	4	Management and Integration	Monitoring, reporting
HIV Voluntary Counselling and Testing (VCT) records	Strictly Confidential	B	SG declassification decision	None	None	HRM	22	Human Resources	Health, welfare
HIV/AIDS programming records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	HUM	8	Humanitarian Affairs	Outreach
Internal audit reports	Confidential	E	Automatic at 20 years	Originator determined	Originator determined	OVE	7	Oversight	Internal Audit
Inter-office vouchers	Unclassified	N/A	Automatic at 20 years	N/A	Mission liquidation	FIN	11	Finance	Inter-office vouchers
Interview transcripts	Public	N/A	N/A	N/A	N/A	PUC	12	Public Information and Communications	External relations
Inventory records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	PRP	8	Property Management	Property control
Invoices	Confidential	A	Automatic at 20 years	Originator determined	Originator determined	FIN	16	Finance	Accounts payable
IT service requests	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	INM	9	Information Management	IT service provision
Joint Disciplinary Committee reports	Strictly Confidential	B	SG declassification decision	None	None	HRM	22	Human Resources	Health, welfare
Judiciary recruitment records	Strictly Confidential	B	SG declassification decision	None	None	JDL	7	Judicial and Legal Systems	Judicial administration
Local Committee on Contracts meeting minutes	Confidential	F	Automatic at 20 years	Originator determined	Originator determined	PRO	8	Procurement and Contracts Management	Contracting: advice
Local government economic development records	Confidential	A	Automatic at 20 years	Originator determined	Originator determined	GOV	9	Governance	Local government capacity building
Local police recruitment records	Strictly Confidential	B	SG declassification decision	None	None	LAE	8	Law Enforcement	Local police administration
Management policies	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	MAT	2	Management and Integration	Policy, procedure
Manifests	Strictly Confidential	B	SG declassification decision	When travel is completed	Originator determined	MOV	9	Movement and Transport	Air transport operation
Medical reports	Strictly Confidential	B	SG declassification decision	None	None	HRM	21	Human Resources	Accidents, casualties
Memoranda of understanding (MoU)	Confidential	A	Automatic at 20 years	Originator determined	MoU rendered obsolete	LEG	7	Legal	Legal agreements development and review

*From ST/SGB/2007/6 Paragraph 1.2
**Peacekeeping File Classification Scheme

ANNEX 17

Records and Possible Security Classifications
For instructional purposes only - Not an exhaustive list

Example records	Possible Security Classification	Caveat*	Declassification Rule	Possible Downgrading Trigger	Possible Declassification Trigger	FCS** Code 1	FCS Code 2	FCS Function	FCS Activity
Military escort records	Strictly Confidential	B	SG declassification decision	When event has passed	Originator determined	MIL	7	Military	Current operations
Military-strategic concept of operations	Confidential	C	Automatic at 20 years	Originator determined	When superseded	MIL	1	Military	Planning, strategy
Mine surveys	Strictly Confidential	B	SG declassification decision	Originator determined	When demining is complete	MIN	7	Mine Action	Mine survey, marking, clearance
Minutes of meetings with host government	Confidential	A	Automatic at 20 years	Originator determined	Originator determined	POL	3	Political Affairs	Coordination, partnership
Micsconduct complaints and case records	Strictly Confidential	B	SG declassification decision	None	None	HRM	20	Human Resources	Administration of justice
Misconduct investigation reports	Strictly Confidential	B	SG declassification decision	None	None	OVE	10	Oversight	Investigation
Mission newsletters	Public	N/A	N/A	N/A	N/A	PUC	7	Public Information and Communications	Publishing
Mission senior management meeting minutes	Confidential	C	Automatic at 20 years	Originator determined	Originator determined	MAT	1	Management and Integration	Planning, strategy
Monthly attendance reports	Strictly Confidential	B	SG declassification decision	None	None	HRM	25	Human Resources	Attendance and leave administration
NOTICAS	Strictly Confidential	B	SG declassification decision	None	None	HRM	21	Human Resources	Accidents, casualties
Occupational safety records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	SAF	12	Safety Management	Occupational safety
Office space planning records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	FEN	10	Facilities and Engineering	Facilities management
Organigrammes	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	HRM	16	Human Resources	Organizational design
Press releases	Public	N/A	N/A	N/A	N/A	PUC	12	Public Information and Communications	External relations
Prisoner rehabilitation records	Strictly Confidential	B	SG declassification decision	None	None	PRC	8	Prisons and Corrections Services	Prisoner reintegration
Property survey case file records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	PRP	10	Property Management	Property survey
Records transfer records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	INM	14	Information Management	Records management
Results-based budgets	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	BUD	8	Budget	Mission budgeting
Security Council resolutions	Public	N/A	N/A	N/A	N/A	POL	6	Political Affairs	Reference
Signed contracts	Confidential	F	Automatic at 20 years	Termination of contract	Originator determined	PRO	9	Procurement and Contracts Management	Contracting: management
SRSG travel itineraries	Strictly Confidential	B	SG declassification decision	When travel is completed	Originator determined	HRM	23	Human Resources	Travel administration
Staff exchange programme records	Strictly Confidential	B	SG declassification decision	None	None	HRM	18	Human Resources	Career development
Staff member's special post allowance records	Strictly Confidential	B	SG declassification decision	None	None	HRM	17	Human Resources	Benefits and entitlements
Staff tracking records	Strictly Confidential	B	SG declassification decision	None	None	SEC	12	Security Management	Staff tracking
Staffing table authorizations	Unclassified	N/A	Automatic at 20 years	N/A	Staffing table superseded	HRM	14	Human Resources	Staffing table management
Status of forces agreements (SOFA)	Confidential	A	Automatic at 20 years	Originator determined	SOFA rendered obsolete	LEG	7	Legal	Legal agreements development and review
Status of mission agreements (SOMA)	Confidential	A	Automatic at 20 years	Originator determined	SOMA rendered obsolete	LEG	7	Legal	Legal agreements development and review
System passwords	Strictly Confidential	B	SG declassification decision	None	None	INM	8	Information Management	IT systems operation
Talking points for a meeting with host government	Confidential	A	Automatic at 20 years	Originator determined	Originator determined	POL	6	Political Affairs	Reference
Testimonies relating to human rights violations	Strictly Confidential	B	SG declassification decision	None	None	HRT	7	Human Rights	Investigation and verification
Theft investigation reports	Confidential	E	Automatic at 20 years	Originator determined	Originator determined	SEC	7	Security Management	Investigation
Training course materials	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	HRM	19	Human Resources	Training
Training placement test results	Strictly Confidential	B	SG declassification decision	None	None	HRM	19	Human Resources	Training
Troop deployment maps	Strictly Confidential	C	SG declassification decision	Map superseded	Originator determined	INM	17	Information Management	Cartography and GI management
Trust fund establishment records	Unclassified	N/A	Automatic at 20 years	N/A	Originator determined	FIN	19	Finance	Trust fund establishment
Vendor quotations	Confidential	F	Automatic at 20 years	Originator determined	Originator determined	PRO	7	Procurement and Contracts Management	Bids, proposals, quotations
Weekly mission situation reports	Confidential	C	Automatic at 20 years	1 month	Originator determined	MAT	4	Management and Integration	Monitoring, reporting

*From ST/SGB/2007/6 Paragraph 1.2
**Peacekeeping File Classification Scheme

ANNEX 17

Justifications for Security Classifying Information (From ST/SGB/2007/6)	
(a) Documents created by the United Nations, received from or sent to third parties, under an expectation of confidentiality;	(e) Internal inter-office or intra-office documents, including draft documents, if disclosure would undermine the Organization's free and independent decision-making process;
(b) Documents whose disclosure is likely to endanger the safety or security of any individual, violate his or her rights or invade his or her privacy;	(f) Documents containing commercial information, if disclosure would harm either the financial interests of the United Nations or those of other parties involved;
(c) Documents whose disclosure is likely to endanger the security of Member States or prejudice the security or proper conduct of any operation or activity of the United Nations, including any of its peacekeeping operations;	(g) Other kinds of information, which because of their content or the circumstances of their creation or communication must be deemed confidential.
(d) Documents covered by legal privilege or related to internal investigations;	