United Nations ST/SGB/2007/6

Secretariat

12 February 2007

Secretary-General's bulletin

Information sensitivity, classification and handling

The Secretary-General, for the purposes of ensuring the classification and secure handling of confidential information entrusted to or originating from the United Nations, promulgates the following:

Section 1
Classification principles

1.1 The overall approach to classifying information entrusted to or originating from the United Nations is based on the understanding that the work of the United Nations should be open and transparent, except insofar as the nature of information concerned is deemed confidential in accordance with the guidelines set out in the present bulletin.

1.2 Information deemed sensitive shall include the following:

(a) Documents created by the United Nations, received from or sent to third parties, under an expectation of confidentiality;

(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;

(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;

(d) Documents covered by legal privilege or related to internal investigations;

(e) Internal inter-office or intra-office documents, including draft documents, if disclosure would undermine the Organization's free and independent decision-making process;

(f) Documents 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 circumstances of their creation or communication must be deemed confidential.

1.3 Classifications should be used judiciously and only in cases where disclosure of the information may be detrimental to the proper functioning of the United

07-23579 (E) 150207

Nations or the welfare and safety of its staff or third parties or violate the Organization's legal obligations. In such cases, the procedures set out below should be strictly observed to ensure that such information is not compromised either purposely or inadvertently.

Section 2
Classification levels

2.1 Sensitive information may be classified as "confidential" or "strictly confidential".

2.2 The designation "confidential" shall apply to information or material whose unauthorized disclosure could reasonably be expected to cause damage to the work of the United Nations.

2.3 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 of the United Nations.

2.4 The designation "unclassified" shall apply to information or material whose unauthorized disclosure could reasonably be expected not to cause damage to the work of the United Nations.

Section 3
Identification and markings

3.1 The originator 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 department or office, shall decide whether the information is sensitive and mark it with the appropriate classification as detailed in section 4 below.

3.2 Where information from an external source contains prior sensitivity markings, it shall retain those markings or shall be assigned a classification that provides a degree of protection greater than or equal to that of the entity that furnished the information.

3.3 The originator 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 department or office, shall, whenever practicable, indicate on the document in question when classified information constitutes a small portion of an otherwise unclassified document.

Section 4
Declassification

4.1 The originator 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 department or office, shall, where appropriate, establish and mark on the document in question a date or an event which will trigger declassification. Upon reaching the date or event, the information shall be declassified automatically. The date or event shall not exceed the time frame established in paragraph 4.3 of this section.

4.2 If no date or event for declassification was specified, information may be declassified at any time by the originator or its recipient if the information is

received from an outside source, by the Secretary-General or by such officials as the Secretary-General so authorizes.

4.3 Review for possible declassification shall take place before records are transferred to the custody of the Archives and Records Management Section, in accordance with Secretary-General's bulletin ST/SGB/2007/5, on record-keeping and the management of United Nations archives. Subject to the provisions of any other applicable administrative rule or any applicable legal undertaking on the part of the Organization, classified records that have been transferred to the Archives and Records Management Section maintaining their original classification, shall be declassified as follows:

(a) Records that are classified as "strictly confidential" shall be reviewed on an item-by-item basis by the Secretary-General, or by such officials as the Secretary-General so authorizes, for possible declassification when 20 years old. Those not declassified at that time shall be further reviewed, every 5 years thereafter, by the Secretary-General or by such officials as the Secretary-General so authorizes, for possible declassification.

(b) Records that are classified as "confidential" shall be declassified automatically by the Archives and Records Management Section when 20 years old.

4.4 When declassifying information received from an outside source, the Organization shall give due regard to expectations of confidentiality of that outside source and, if appropriate, shall seek the prior consent of the outside source.

Section 5
Handling of classified information

5.1 Heads of departments or offices shall ensure that the following minimal standards are maintained in the handling of classified information received by or originating from their department or office:

(a) All classified information must be transported in sealed envelopes or containers, and clearly marked as such;

(b) All outgoing and incoming classified information must be recorded in a special registry that lists the staff members who are authorized to handle such information;

(c) Classified materials may be duplicated only with the authorization of either their originator or the head of the receiving or originating department or office, and such copies must be entered in the special registry;

(d) All classified information must be filed and stored under lock and key in a secure location within the department or office concerned, accessible only to the authorized staff members;

(e) A hard copy of classified information received in an electronic form must be printed when received, and filed and stored as detailed in subparagraph (d) above. The electronic file must be securely stored in accordance with section 5.4 below;

(f) Electronic transmission of classified information shall be performed only through the use of protected means of communication, in accordance with section 5.4 below.

5.2 With regard to classified information of a recurrent nature (such as situation reports, operational updates and periodic political assessments), departments or offices shall establish standard distribution lists to provide an auditable system for the distribution and control of such information.

5.3 The above minimum standards are without prejudice to the authority of heads of departments or offices to put in place stricter controls over the handling of classified information so long as such controls are consistent with the present bulletin.

5.4 Heads of departments and offices, in cooperation with the Information Technology Services Division of the Department of Management, shall establish procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process or store classified information, have controls that both prevent access by unauthorized persons, and ensure the integrity of the information.

5.5 The destruction by authorized means of non-current, classified documents that have no further administrative, fiscal, legal, historical or other informational value shall be authorized either by the originator or the head of the department or office concerned.

Section 6
Final provisions

6.1 The provisions of the present bulletin shall not apply to the classification and handling of records specifically covered in other Secretary-General's bulletins, other administrative issuances promulgated by the Secretary-General or legal undertakings made by the Organization to third parties.

6.2 Secretary-General's bulletin ST/SGB/272, on security of information, and administrative instruction ST/AI/189/Add.16, on regulations for the control and limitation of documentation: classification and declassification of documents, are hereby abolished.

6.3 The present bulletin shall enter into force on 15 February 2007.

(*Signed*) **Ban** Ki-moon
Secretary-General