United Nations
Climate Change Secretariat

Nations Unies
Secrétariat sur les changements climatiques

SECRETARIAT BULLETIN **B/2012/2**

1 November 2012

Information sensitivity, classification and handling

Purpose

1. The purpose of this bulletin is to implement the United Nations Secretary-General's Bulletin ST/SGB/2007/6 on Information sensitivity, classification and handling within the UNFCCC secretariat.

2. Work instructions on the implementation of the policy are contained in administrative guidelines issued separately.

Guiding principles

3. In line with the United Nations principles, regulations, rules, and procedures, the overall approach to classifying information entrusted to or originating from the secretariat is based on the understanding that the work of the secretariat should be open and transparent, except insofar as the nature of information concerned is deemed sensitive.

4. At the same time, the secretariat works in a highly political and dynamic environment in which the sharing of information not intended for external audiences can have serious consequences for the UNFCCC process, Parties, stakeholders and for the reputation of the secretariat.

5. It is incumbent upon each staff member to exercise careful judgement in deciding how to treat sensitive information. If in doubt as to how to classify certain information and whether it should be shared with others, internally or externally, staff must consult their supervisor for guidance.

6. Staff members who, by virtue of their responsibilities or roles, have access to sensitive information are duty-bound to keep that information confidential. Such information must not be shared with others, nor should they be asked by others to share it, without permission from the supervisor. This is a matter of professional responsibility and integrity of all secretariat staff members.

7. Under the United Nations Oath of Office, staff members have pledged to exercise in all loyalty, discretion and conscience the functions entrusted to them as an international civil servant of the United Nations. Discretion and careful judgement are essential, in particular in situations where staff members, as part of their professional roles, are requested to obtain information from or share information with Parties and other stakeholders.

8. Staff are reminded that disciplinary procedures set out in Article X of the United Nations Staff Regulations and Rules may be instituted against a staff member who fails to comply with his or her obligations and the standards of conduct set out in the Charter of the United Nations, the United Nations Staff Regulations and Staff Rules as well as in the United Nations and UNFCCC policies and administrative guidelines, including the guidelines on information sensitivity, classification and handling.

Implementation of UN ST/SGB/2007/6, "Information sensitivity, classification and handling"

9. ST/SGB/2007/6 will be implemented at the secretariat with adjustments to sections 1.2 (g), 3.1, 3.3, 4.1, 4.2, 4.3, 4.3 (a) and (b), 5.1, 5.1 (b), (c) and (e), 5.2, 5.3, 5.4 and 5.5 as outlined in the paragraphs hereunder, to reflect the particular institutional setting of the UNFCCC secretariat.

10. Procedures, guidelines and work instructions issued separately will elaborate on the nature of "other kinds of information" mentioned in section 1.2 (g).

11. References to "head[s] of department[s] or office[s]" in sections 3.1, 3.3, 4.1, 5.1, 5.3, 5.4 and 5.5 shall mean the "Head of programme", such as the Director or Coordinator.

12. All references to "Secretary General" in section 4.2 and 4.3 (a) shall mean the "Executive Secretary."

13. References to "departments or offices" in section 5.1 and 5.2 shall mean "Programmes."

14. Section 4.3 of ST/SGB/2007/6 shall be amended as follows:
"Review for possible declassification shall take place before records are transferred to the custody of the Knowledge Management Unit, in accordance with Secretariat Bulletin Amendment No. 1B/2007/2-Amend.1, UNFCCC Policy for Records and 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 Knowledge Management Unit maintaining their original classification, shall be declassified as follows:"

15. Reference to the "Archives and Records Management Section" in 4.3 (b) shall mean the "Knowledge Management Unit."

16. Section 5.1 (b) and (c) are not applicable.

17. Section 5.1 (e) shall be replaced by the following provision: "Electronic records which contain sensitive information shall be captured into UNFCCC's central recordkeeping system if available to the programme or unit. Where it is not available, programmes shall work with CKM and ITS to establish secure retention of the information. Documents secured into the central recordkeeping system must be deleted from private drives and email systems."

18. Additional paragraphs in 5.1 re handling:

    a. Staff shall not copy sensitive information unless absolutely necessary and shall protect any such sensitive information from unauthorized access and destroy it as soon as no longer needed;
    b. Former staff members are prohibited from disclosing all sensitive information except with advance written consent from the secretariat;
    c. Staff are prohibited from sharing information contained in sensitive documents to unauthorised persons in either private or professional capacities.

19. Reference to the "Technology Services Division of the Department of Management" in section 5.4 shall mean "Information Technology Services Programme and Communications and Knowledge Management Services Programme."

Roles and responsibilities

A. Executive Secretary (ES)

20. The Executive Secretary has overall accountability for the implementation of this bulletin and related guidelines to ensure the safeguarding of sensitive information at the secretariat.

B. Deputy Executive Secretary (DES)

21. On behalf of the ES, the DES shall oversee the implementation of this bulletin and related guidelines on information sensitivity, classification and handling. He/she is assisted in this effort by the MT sub-committee on Ethics.

C. Communications and Knowledge Management Services (CKMS)

22. CKMS, within assigned resources, shall provide technical expertise in developing guidelines and supporting programmes in the implementation of the bulletin and relevant administrative guidelines on sensitive information classification and handling of sensitive information. CKMS shall assist the DES in overseeing policy implementation by providing information or recommendations as requested and raising issues that may require senior management intervention.

23. CKMS shall, in coordination with AS and programme focal points, facilitate awareness training of staff on information sensitivity, classification and handling;

24. CKMS shall, in close coordination with programmes, support the development of the programme specific work instructions when required;

25. CKMS shall, in consultation with programmes, maintain the secretariat sensitive information asset register.

D. Heads of Programme

26. Heads of Programme shall ensure that the sensitive information created, received and handled in their programme is identified, classified, marked, protected and managed in accordance with this bulletin and related guidelines on information sensitivity, classification and handling.

27. Heads of programme shall ensure that information and assistance is provided to CKMS, as required, for CKMS to effectively assist in:

    a. Identifying and classifying the sensitive information received or created in their offices;
    b. Developing guidelines and programme-specific work instructions relating to information sensitivity, classification and handling;
    c. Developing and maintaining the programme sensitive information asset list;
    d. Developing knowledge management business requirements.

28. Heads of Programmes shall ensure that:

    a. Staff are trained on work instructions relating to information sensitivity, classification and handling specific to their programme;
    b. Staff capture electronic records which contain sensitive information into the secretariat's central recordkeeping system, if available to the programme or unit;

c. Sensitive information is disposed of when no longer needed in a timely and secure way and in compliance with the information policy and the records retention schedule;
d. Inactive or permanent physical records of sensitive information are transferred to CKMS for long-term storage.

29. Heads of programmes shall ensure that information and assistance is provided to ITS, as required, for ITS to effectively assist in:

a. Identification and definition of information technology services requirements for the protection of sensitive information;
b. Implementation and maintenance of information technology services to meet those requirements;
c. Assessment of residual risk resulting from the use of information systems to protect sensitive information in accordance with the secretariat's policies on information sensitivity, classification and handling.

30. Heads of programmes need to be aware of and explicitly accept any residual risks related to protecting sensitive information.

E. Administrative Services (AS)

31. AS shall ensure that all staff members sign the secretariat staff undertaking on avoidance of conflict of interest and safeguarding confidentiality.

32. AS shall provide the necessary administrative support for the training of staff on information sensitivity, classification and handling, including the induction training modules and other secretariat-wide general training.

F. Information Technology Services (ITS)

33. ITS shall, within assigned resources, ensure that appropriate information technology services are in place such that sensitive information that is stored, captured or communicated electronically by or with the secretariat can be protected in accordance with the secretariat's policies on information sensitivity, classification and handling.

34. ITS shall, within assigned resources, advise the secretariat and programmes on the information technology services required to protect sensitive information in accordance with the secretariat's policies on information sensitivity, classification and handling, the financial and human resources required to implement and maintain such services, and residual risk resulting from the secretariat's use of information technology services for this purpose.

G. Staff

35. Staff members shall ensure that sensitive information they create and receive during their business activity is identified and classified at the appropriate level and is managed in accordance with that classification irrespective of format or transmission method, including verbal communication;

36. Staff members shall consult their immediate supervisor for advice if in doubt or unable to comply with the secretariat's policies on information sensitivity, classification and handling.

Final Provisions

37. The present bulletin shall enter into force on 1 January 2013.

(signed) Christiana Figueres
Executive Secretary