International Seabed Authority ISBA/ST/SGB/2011/03

# Secretariat

28 January 2011

Original: English

## Secretary-General's bulletin

To: Members of the staff

From: The Secretary-General

Subject: **Information sensitivity, classification and handling**

The purpose of the present bulletin is to establish procedures to ensure the appropriate classification and secure handling of confidential data and information entrusted to or originating from the International Seabed Authority ("the Authority"), with a view to implementing article 168 of the United Nations Convention on the Law of the Sea ("the Convention") and the rules, regulations and procedures of the Authority relating to prospecting and exploration in the Area ("the Regulations") .

### Section 1
### Scope

1. The provisions of the present bulletin are in principle applicable to all data and information entrusted to or originating from the Authority regardless of their source or destination.

2. In the case of data and information submitted or transferred to the Authority or to any person participating in any activity or programme of the Authority pursuant to the Regulations or a contract issued under the Regulations, the Secretary-General shall be responsible for maintaining the confidentiality of all such data and information in accordance with the Regulations. To this end, the Secretary-General shall establish procedures, consistent with the provisions of the Convention, governing the handling of confidential information. Additional procedures for this purpose are set out in annex II.

13-35080 (E) 200613

## Section 2
## Record-keeping and the management of the archives of the Authority

***Definitions***

4. The following definitions shall apply for the purposes of the present bulletin:

(a) Archives: records to be permanently preserved for their administrative, fiscal, legal, historical or informational value;

(b) Disposition: the action taken with regard to non-current records following their appraisal, including transfer to secondary storage, or destruction;

(c) ICT data: any data or information, regardless of form or medium, which are or have been electronically generated by, transmitted via, received by, processed by or represented in an information and communication technology resource (ICT resource), such as e-mail and facsimile systems;

(d) Non-current record: any data or information no longer needed for daily use in the transaction of official business but to be retained for a fixed period of time;

(e) Official use: use of ICT resources by an authorized user in the discharge of his or her official functions and within the scope of his or her authorization;

(f) Record (or official record): any data or information, regardless of form or medium, maintained by the Authority as evidence of a transaction;

(g) Record-keeping: making, maintaining and disposing of complete, accurate and reliable evidence of transactions in the form of records;

(h) Retention schedule: a comprehensive instruction developed by an office covering the disposition of records to ensure that they are retained for as long as necessary based on their administrative, fiscal, legal, historical or informational value;

(i) Transaction: act by a staff member using an ICT resource in the discharge of his or her official functions;

(j) Transitory record: any data or information required for only a limited time to ensure the completion of a routine action or the preparation of a subsequent record;

(k) Vital record: any data or information essential for the ongoing functioning of the Authority and without which the Authority could not continue to function effectively or without which it could not ensure business continuity in the event of a disaster; information necessary to protect the rights and interests of the Authority, its staff and those who interact with it.

***Responsibilities of staff members***

5. All records, including electronic records and e-mail records, created or received by a staff member in connection with or as a result of the official work of the Authority, are the property of the Authority.

6. Staff members shall not alter, destroy, misplace or render useless any official document, record or file that is intended to be kept as a record of the Authority. Staff members are permitted to destroy documents and records in keeping with the provisions of retention policy guidelines that have been approved by the Secretary-General.

7. Prior to separation from service, staff members shall make arrangements for transferring to their respective office those records in their possession which are no longer required for business purposes and shall not remove any records from Authority's premises. The head of each office may provide advice regarding the records of a staff member prior to separation from service. Staff members shall be entitled to have a reasonable number of unrestricted records copied at their own expense and to retain their private papers.

8. The following categories of records are considered private papers of staff members:

(a) Personal notes and diaries;

(b) Surplus copies of non-classified printed documents of the Authority;

(c) Personal correspondence with no connection to a staff member's official functions, even though filed in a Secretariat office, including social invitations, acknowledgements, correspondence lists and other purely social matters.

9. Upon retirement, staff members may remove the private papers specified in paragraph 8 above.

***Responsibilities of offices***

10. Each office shall develop and implement a policy regarding the retention of their records, including transitory records, through a records retention schedule subject to approval by the Secretary-General. Records retention schedules shall provide for accountable and transparent record-keeping, insofar as they shall identify minimum retention periods for records to meet administrative, fiscal and legal requirements; they shall also identify records to be retained as archives of the Authority. Authority's records that are not covered by an approved retention policy must not be destroyed.

11. Prior to transferring their records to the archives of the Authority, each office shall prepare them for transfer in accordance with the format established by the Secretary-General.

12. With the exception of transitory records, offices may not dispose of records in their possession without specific authorization in a retention schedule or the signed authorization of the Secretary-General.

13. Each office authorized to retain non-current records beyond the normal period for the conduct of their official business shall establish suitable conditions for the maintenance and preservation of those records, in accordance with standards approved by the Secretary-General.

14. Each office shall develop procedures to identify and manage their vital records as part of overall Secretariat disaster recovery and business continuity planning, in keeping with the guidelines to identify vital records established by the Secretary-General.

***Electronic records***

15. Electronic records created or managed using an Authority ICT resource shall be subject to the requirements for record-keeping set forth in the present bulletin, including their capture in electronic record-keeping systems; if such a system is not yet available, electronic records must be captured and maintained in an alternative record-keeping system, for example, one that is paper-based.

16. Many of the e-mail messages created and received by the Authority constitute records because they provide evidence of and information about its business transactions. Each office shall ensure that e-mail records are identified, managed and stored in accordance with the requirements for record-keeping set forth in the present bulletin. The Information Technology Manager ("IT Manager") shall develop and disseminate guidelines, in keeping with business process and practice, to prescribe appropriate use of e-mail systems as a means of official communication.

***Access of staff members to Authority's archives and non-current records***

17. Staff members shall have access to archives and non-current records necessary to conduct their official business, subject to the terms and conditions established by the Secretary-General.

18. Records, other than data and information submitted pursuant to the Regulations, which shall be dealt with in accordance with the provisions of the Regulations and annex II of the present bulletin, on which the Secretary-General or his authorized representatives have imposed restrictions may be declassified at any time by the same authority.

## Section 3
## Information sensitivity, classification and handling

***Classification principles***

19. The overall approach to classifying information entrusted to or originating from the Authority is based on the understanding that the work of the Authority 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.

20. Information deemed sensitive shall include the following:

(a) Documents created by the Authority, 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 covered by legal privilege or related to internal investigations;

(d) Internal inter-office or intra-office documents, including draft documents, which if disclosed would undermine the Authority's free and independent decision-making process;

(e) Documents containing commercial information, which if disclosed would harm either the financial interests of the Authority or those of other parties involved;

(f) Data and information submitted pursuant to the Regulations;

(g) Other kinds of information, which because of their content or the circumstances of their creation or communication must be deemed confidential.

21. Classifications should be used judiciously and only in cases where disclosure of the information may be detrimental to the proper functioning of the Authority or the welfare and safety of its staff or third parties or violate the Authority'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.

***Classification levels***

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

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

24. 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 interest of a member State or a contractor or applicant for a contract with the Authority and conduct of the work of the Authority. Data and information deemed confidential pursuant to the Regulations shall always be considered "strictly confidential" unless otherwise decided by the Secretary-General.

25. 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 Authority.

***Identification and markings***

26. 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 office, shall decide whether the information is sensitive and mark it with the appropriate classification as detailed below.

27. 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.

28. 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 office, shall, whenever practicable, indicate on the document in question when classified information constitutes a small portion of an otherwise unclassified document.

***Declassification***

29. 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 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 31 below.

30. 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.

31. Subject to the provisions of any other applicable administrative rule or any applicable legal undertaking on the part of the Authority, classified records that have been transferred to the Secretary-General 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 10 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, subject, in the case of confidential data and information submitted pursuant to a contract for exploration, to the relevant provisions of the Regulations;

(b) Records that are classified as "confidential" shall be declassified automatically by Secretary-General when 10 years old, subject in the case of confidential data and information submitted pursuant to a contract for exploration, to the relevant provisions of the Regulations.

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

***Handling of classified information***

33. Heads of offices shall ensure that the following minimal standards are maintained in the handling of classified information received by or originating from their 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 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 office concerned, accessible only staff members authorized by the head of office;

(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 paragraph 36 below;

(f) Electronic transmission of classified information shall be performed only through the use of protected means of communication, in accordance with paragraph 36 below.

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

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

36. Heads of offices, in cooperation with the IT Manager, 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.

37. 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 office concerned.

## Section 4
## Basic obligations of staff members and disciplinary measures for violations thereof

***Basic obligations***

38. The basic obligations of staff members with respect to the confidentiality of information and data as provided under the Convention, the Staff Regulations and Rules, and the Regulations include the following:

(a) Staff members shall not use their office or knowledge gained from their official functions for private gain, financial or otherwise, or for the private gain of any third party, including family, friends and those they favour.

(b) Staff members shall exercise the utmost discretion in regard to all matters of official business. They shall not communicate to any government, entity, person or any other source any information known to them by reason of their official position that they know or ought to have known has not been made public, except as appropriate in the course of their duties or by authorization of the Secretary-General. These obligations do not cease upon separation from service.

(c) In accordance with article 168, paragraph 2, of the Convention, subject to their responsibilities to the Authority, the Secretary-General and the staff shall not

disclose, even after the termination of their functions, any industrial secret, proprietary data which are transferred to the Authority in accordance with Annex III, article 14, or any other confidential information coming to their knowledge by reason of their employment with the Authority.

(d) Heads of office and staff members shall promptly report to the Secretary-General any violation of the provisions of this section.

39. Failure by a staff member to comply with his or her obligations as set out in the present bulletin may amount to unsatisfactory conduct within the meaning of Staff Regulation 10.2 leading to the institution of disciplinary proceedings and the imposition of disciplinary measures for misconduct.

40. Without prejudice to the provisions of Chapter X of the Staff Rules, the following procedures shall apply to any alleged breach of the provisions of this bulletin relating to confidentiality.

***Initial investigation and fact-finding***

41. Where there is reason to believe that a staff member has failed to comply with his or her obligations under the present bulletin the head of office or responsible officer shall undertake a preliminary investigation.

42. If the preliminary investigation appears to indicate that the report is well founded, the head of office or responsible officer should immediately report the matter to the Secretary-General, giving a full account of the facts that are known and attaching documentary evidence.

43. If the conduct appears to be of such a nature and of such gravity that suspension may be warranted, the head of office or responsible officer shall make a recommendation to that effect, giving reasons. As a general principle, suspension may be contemplated if the conduct in question might pose a danger to other staff members or to the Authority, or if there is a risk of evidence being destroyed or concealed and if redeployment is not feasible.

44. On the basis of the evidence presented, the Secretary-General shall decide whether the matter should be pursued, and, if so, whether suspension is warranted. Suspension under staff rule 110.2 (a) is normally with pay, unless the Secretary-General decides that exceptional circumstances warrant suspension without pay.

***Monitoring and investigation conducted by IT Manager***

45. Technical monitoring of the use of ICT resources is routinely performed for troubleshooting, diagnostics, statistical analysis and performance tuning. This may include the compiling of aggregated data for a general monitoring of usage.

46. The IT Manager shall conduct an investigation upon request from the Secretary-General.

(a) Requests for investigation in this section of the use of ICT resources shall be addressed to the Secretary-General. Such requests shall be made in writing and provide a brief description of the data required, the name of the staff member or other individual to be investigated and the name of the authorized official from the requesting office to whom the records are to be delivered;

(b) The investigation shall begin only after the Secretary-General has approved the request for investigation;

47. The following procedures shall apply in cases of such investigations:

(a) Staff members and their supervisors shall be informed immediately preceding access to their ICT resources or ICT data, including electronic files, e-mail and Intranet/Internet access records, by the office conducting the investigation;

(b) Whenever practicable, physical investigations involving ICT resources or ICT data shall be performed in the presence of the staff member, his or her supervisor and a representative from the requesting office;

(c) If necessary to ensure the integrity of the investigation, the staff member may be denied access to the ICT resources and ICT data under investigation, including computers, electronic files and e-mail accounts;

(d) The authorized official of the requesting office shall be required to sign a note confirming receipt of any data retrieved;

(e) A special register shall be maintained in a secure location by the IT Manager, recording a brief description of the request for investigation, the requestor's name, the activities undertaken in carrying out the investigation, the name of the personnel performing such activities and the type of information retrieved and provided to the requester;

(f) The data retrieved and provided to the requester shall not be retained by IT Manager. The original signed written request and receipt for any data provided to the requesting office shall be kept in a separate file in a secure location in the Office of the Secretary-General;

(g) Monitoring or investigation shall continue for only so long as is reasonably necessary to ascertain whether the suspected misconduct has occurred. If no further action will be taken in regard to such suspected violation, the staff member involved shall be so informed by the office that requested such monitoring or investigation.

***Notification to the staff member of the result of the investigation***

48. If a case is to be pursued, the Secretary-General shall:

(a) Inform the staff member in writing of the allegations and his or her right to respond;

(b) Provide him or her with a copy of the documentary evidence of the alleged misconduct;

(c) Notify the staff member of his or her right to the advice of another staff member or retired staff member to assist in his or her responses; and offer information on how to obtain such assistance.

49. If the Secretary-General authorizes suspension, the staff member shall be informed of the reason for the suspension and its probable duration and shall surrender his or her grounds pass. A staff member on suspension may not enter the Authority's premises without first requesting permission and shall be afforded the opportunity to enter, under escort, if necessary to prepare his or her defence or for any other valid reason.

50. The staff member should be given a specified time to answer the allegations and produce countervailing evidence, if any. The amount of time allowed shall take account of the seriousness and complexity of the matter. If more time is required, it shall be granted upon the staff member's written request for an extension, giving cogent reasons why he or she is unable to comply with the deadline. If no response is submitted within the time-limit, the matter shall nevertheless proceed.

51. The entire dossier will then be submitted to the Secretary-General. It shall consist of the documentation listed under paragraphs 48 above, the staff member's reply and the evidence, if any, that he or she has produced.

52. On the basis of the entire dossier, the Secretary-General shall proceed as follows:

(a) Decide that the case should be closed, and the staff member should be immediately notified that the allegations have been dropped and that no further action will be taken. This is without prejudice, where appropriate, to the measures indicated in staff rule 110.3 (b) (i) and (ii); or

(b) Should the facts appear to indicate that misconduct has occurred, refer the matter to the Joint Disciplinary Committee for advice; or

(c) Should the evidence clearly indicate that misconduct has occurred, and that the seriousness of the misconduct warrants immediate separation from service, decides that the staff member be summarily dismissed.

53. All disciplinary proceedings shall be taken in accordance with the provisions of Chapter X of the Staff Rules.

54. Violation of the obligations of a staff member set forth in article 168, paragraph 2, of the Convention shall, on the request of a State party to the Convention affected by such violation, or natural or judicial person sponsored by a State party as provided in article 153, paragraph 2(b), of the Convention and affected by such violation, be submitted by the Authority against the staff member concerned to an ad hoc tribunal of three qualified persons appointed by the Secretary-General of the United Nations. The party affected shall have the right to take part in the proceedings. If the tribunal so recommends, the Secretary-General shall dismiss the staff member concerned.

## Section 5
## Final provisions

55. 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 Authority to third parties.

56. The present bulletin shall enter into force on 1 February 2011.

- - -

# Annex I

## Relevant provisions of the Convention and the Regulations

### United Nations Convention on the Law of the Sea

*Article 168*
*International character of the Secretariat*

1. In the performance of their duties the Secretary-General and the staff shall not seek or receive instructions from any government or from other source external to the Authority. They shall refrain from any action which might reflect on their position as international officials responsible only to the Authority. Each State party undertakes to respect the exclusively international character of the responsibilities of the Secretary-General and the staff and not to seek to influence them in the discharge of their responsibilities. Any violation of the responsibilities by a staff member shall be submitted to the appropriate administrative tribunal as provided in the rules, regulations and procedures of the Authority.

2. The Secretary-General and the staff shall have no financial interest in any activity relating to exploration and exploitation in the Area. Subject to their responsibilities to the Authority, they shall not disclose, even after the termination of their functions, any industrial secret, proprietary data which are transferred to the Authority in accordance with Annex III, article 14, or any other confidential information coming to their knowledge by reason of their employment with the Authority.

3. Violations of the obligations of a staff member of the Authority set forth in paragraph 2 shall, on the request of a State Party affected by such violation, or a natural or juridical person, sponsored by a State Party as provided in article 153, paragraph 2(b), and affected by such violation, be submitted by the Authority against the staff member concerned to a tribunal designated by the rules, regulations and procedures of the Authority. The party affected shall have the right to take part in the proceedings. If the tribunal so recommends, the Secretary-General shall dismiss the staff member concerned.

4. The rules, regulations and procedures of the Authority shall contain such provisions as are necessary to implement this article.

*Annex III*
*Article 14*
*Transfer of data*

1. The operator shall transfer to the Authority, in accordance with its rules, regulations and procedures and the terms and conditions of the plan of work, at time intervals determined by the Authority all data which are both necessary for and relevant to the effective exercise of the powers and functions of the principal organs of the Authority in respect of the area covered by the plan of work.

2. Transferred data in respect of the area covered by the plan of work, deemed proprietary, may only be used for the purposes set forth in this article. Data necessary for the formulation by the Authority of rules, regulations and procedures concerning protection of the marine environment and safety, other than equipment design data, shall not be deemed proprietary.

3. Data transferred to the Authority by prospectors, applicants for contracts or contractors, deemed proprietary, shall not be disclosed by the Authority to the Enterprise or to anyone external to the Authority, but data on the reserved areas may be disclosed to the Enterprise. Such data transferred by such persons to the Enterprise shall not be disclosed by the Enterprise to the Authority or to anyone external to the Authority.

## Regulations on prospecting and exploration for polymetallic nodules in the Area

*Regulation 35*
*Proprietary data and information and confidentiality*

1. Data and information submitted or transferred to the Authority or to any person participating in any activity or programme of the Authority pursuant to these Regulations or a contract issued under these Regulations, and designated by the contractor, in consultation with the Secretary-General, as being of a confidential nature, shall be considered confidential unless it is data and information which:

(a) is generally known or publicly available from other sources;

(b) has been previously made available by the owner to others without an obligation concerning its confidentiality; or

(c) is already in the possession of the Authority with no obligation concerning its confidentiality.

2. Confidential data and information may only be used by the Secretary-General and staff of the Secretariat, as authorized by the Secretary-General, and by the members of the Legal and Technical Commission as necessary for and relevant to the effective exercise of their powers and functions. The Secretary-General shall authorize access to such data and information only for limited use in connection with the functions and duties of the staff of the Secretariat and the functions and duties of the Legal and Technical Commission.

3. Ten years after the date of submission of confidential data and information to the Authority or the expiration of the contract for exploration, whichever is the later, and every five years thereafter, the Secretary-General and the contractor shall review such data and information to determine whether they should remain confidential. Such data and information shall remain confidential if the contractor establishes that there would be a substantial risk of serious and unfair economic prejudice if the data and information were to be released. No such data and information shall be released until the contractor has been accorded a reasonable opportunity to exhaust the judicial remedies available to it pursuant to Part XI, section 5, of the Convention.

4. If, at any time following the expiration of the contract for exploration, the contractor enters into a contract for exploitation in respect of any part of the exploration area, confidential data and information relating to that part of the area shall remain confidential in accordance with the contract for exploitation.

5. The contractor may at any time waive confidentiality of data and information.

*Regulation 36*
*Procedures to ensure confidentiality*

1. The Secretary-General shall be responsible for maintaining the confidentiality of all confidential data and information and shall not, except with the prior written consent of the contractor, release such data and information to any person external to the Authority. To ensure the confidentiality of such data and information, the Secretary-General shall establish procedures, consistent with the provisions of the Convention, governing the handling of confidential information by members of the Secretariat, members of the Legal and Technical Commission and any other person participating in any activity or programme of the Authority. Such procedures shall include:

(a) maintenance of confidential data and information in secure facilities and development of security procedures to prevent unauthorized access to or removal of such data and information;

(b) development and maintenance of a classification, log and inventory system of all written data and information received, including its type and source and routing from the time of receipt until final disposition.

2. A person who is authorized pursuant to these Regulations to have access to confidential data and information shall not disclose such data and information except as permitted under the Convention and these Regulations. The Secretary-General shall require any person who is authorized to have access to confidential data and information to make a written declaration witnessed by the Secretary-General or his or her authorized representative to the effect that the person so authorized:

(a) acknowledges his or her legal obligation under the Convention and these Regulations with respect to the non-disclosure of confidential data and information;

(b) agrees to comply with the applicable regulations and procedures established to ensure the confidentiality of such data and information.

3. The Legal and Technical Commission shall protect the confidentiality of confidential data and information submitted to it pursuant to these Regulations or a contract issued under these Regulations. In accordance with the provisions of article 163, paragraph 8, of the Convention, members of the Commission shall not disclose, even after the termination of their functions, any industrial secret, proprietary data which are transferred to the Authority in accordance with Annex III, article 14, of the Convention, or any other confidential information coming to their knowledge by reason of their duties for the Authority.

4. The Secretary-General and staff of the Authority shall not disclose, even after the termination of their functions with the Authority, any industrial secret, proprietary data which are transferred to the Authority in accordance with Annex III, article 14, of the Convention, or any other confidential information coming to their knowledge by reason of their employment with the Authority.

5. Taking into account the responsibility and liability of the Authority pursuant to Annex III, article 22, of the Convention, the Authority may take such action as may be appropriate against any person who, by reason of his or her duties for the Authority, has access to any confidential data and information and who is in breach of the obligations relating to confidentiality contained in the Convention and these Regulations.

## Regulations on prospecting and exploration for polymetallic sulphides in the Area

*Regulation 38*
*Proprietary data and information and confidentiality*

1. Data and information submitted or transferred to the Authority or to any person participating in any activity or programme of the Authority pursuant to these Regulations or a contract issued under these Regulations, and designated by the contractor, in consultation with the Secretary-General, as being of a confidential nature, shall be considered confidential unless it is data and information which:

(a) is generally known or publicly available from other sources;

(b) has been previously made available by the owner to others without an obligation concerning its confidentiality; or

(c) is already in the possession of the Authority with no obligation concerning its confidentiality.

2. Confidential data and information may only be used by the Secretary-General and staff of the Secretariat, as authorized by the Secretary-General, and by the members of the Legal and Technical Commission as necessary for and relevant to the effective exercise of their powers and functions. The Secretary-General shall authorize access to such data and information only for limited use in connection with the functions and duties of the staff of the Secretariat and the functions and duties of the Legal and Technical Commission.

3. Ten years after the date of submission of confidential data and information to the Authority or the expiration of the contract for exploration, whichever is the later, and every five years thereafter, the Secretary-General and the contractor shall review such data and information to determine whether they should remain confidential. Such data and information shall remain confidential if the contractor establishes that there would be a substantial risk of serious and unfair economic prejudice if the data and information were to be released. No such data and information shall be released until the contractor has been accorded a reasonable opportunity to exhaust the judicial remedies available to it pursuant to Part XI, section 5, of the Convention.

4. If, at any time following the expiration of the contract for exploration, the contractor enters into a contract for exploitation in respect of any part of the exploration area, confidential data and information relating to that part of the area shall remain confidential in accordance with the contract for exploitation.

5. The contractor may at any time waive confidentiality of data and information.

*Regulation 39*
*Procedures to ensure confidentiality*

1. The Secretary-General shall be responsible for maintaining the confidentiality of all confidential data and information and shall not, except with the prior written consent of the contractor, release such data and information to any person external to the Authority. To ensure the confidentiality of such data and information, the Secretary-General shall establish procedures, consistent with the provisions of the Convention, governing the handling of confidential information by members of the

Secretariat, members of the Legal and Technical Commission and any other person participating in any activity or programme of the Authority. Such procedures shall include:

(a) maintenance of confidential data and information in secure facilities and development of security procedures to prevent unauthorized access to or removal of such data and information;

(b) development and maintenance of a classification, log and inventory system of all written data and information received, including its type and source and routing from the time of receipt until final disposition.

2. A person who is authorized pursuant to these Regulations to have access to confidential data and information shall not disclose such data and information except as permitted under the Convention and these Regulations. The Secretary-General shall require any person who is authorized to have access to confidential data and information to make a written declaration witnessed by the Secretary-General or his or her authorized representative to the effect that the person so authorized:

(a) acknowledges his or her legal obligation under the Convention and these Regulations with respect to the non-disclosure of confidential data and information;

(b) agrees to comply with the applicable regulations and procedures established to ensure the confidentiality of such data and information.

3. The Legal and Technical Commission shall protect the confidentiality of confidential data and information submitted to it pursuant to these Regulations or a contract issued under these Regulations. In accordance with the provisions of article 163, paragraph 8, of the Convention, members of the Commission shall not disclose, even after the termination of their functions, any industrial secret, proprietary data which are transferred to the Authority in accordance with Annex III, article 14, of the Convention, or any other confidential information coming to their knowledge by reason of their duties for the Authority.

4. The Secretary-General and staff of the Authority shall not disclose, even after the termination of their functions with the Authority, any industrial secret, proprietary data which are transferred to the Authority in accordance with Annex III, article 14, of the Convention, or any other confidential information coming to their knowledge by reason of their employment with the Authority.

5. Taking into account the responsibility and liability of the Authority pursuant to Annex III, article 22, of the Convention, the Authority may take such action as may be appropriate against any person who, by reason of his or her duties for the Authority, has access to any confidential data and information and who is in breach of the obligations relating to confidentiality contained in the Convention and these Regulations.

- - -

# Annex II

## Additional procedures for the handling of data and information submitted or transferred to the Authority pursuant to annex III of the Convention and the Regulations

### Application and scope

1. The provisions of this annex apply in addition to the general procedures outlined in the present bulletin.

2. The provisions of this annex apply specifically to data and information submitted or transferred to the Authority or to any person participating in any activity or programme of the Authority pursuant to the Regulations or a contract issued under the Regulations. In accordance with the Regulations, this annex makes provision for:

(a) maintenance of confidential data and information in secure facilities and development of security procedures to prevent unauthorized access to or removal of such data and information;

(b) development and maintenance of a classification, log and inventory system of all written data and information received, including its type and source and routing from the time of receipt until final disposition.

3. Data and information covered by this annex shall be considered confidential unless they are data and information which:

(a) are generally known or publicly available from other sources;

(b) have been previously made available by the owner to others without an obligation concerning its confidentiality; or

(c) are already in the possession of the Authority with no obligation concerning its confidentiality.

4. The Secretary-General shall ensure the secure treatment of all data and information referred to in paragraph 2. In particular, the Secretary-General shall implement appropriate technical and organizational measures as described herein to protect such data and information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all inappropriate forms of processing. Having regard to the state of art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing of these data and information, and shall address the following issues:

(a) System access control: the system has to withstand a break-in attempt from unauthorized persons.

(b) Authenticity and data access control: the system has to be able to limit the access of authorized parties to a predefined set of data only.

(c) Communication security: It shall be guaranteed that all data and information are securely communicated.

(d) Data security: It has to be guaranteed that all data and information that enter the system are securely stored for the required time and that they will not be tampered with.

(e) Security procedures: Security procedures shall be designed addressing access to the system (both hardware and software), system administration and maintenance, backup and general usage of the system.

**General security procedures**

4. All data and information covered by this annex, whether in hard copy or electronic format shall be kept in safe custody under the authority of the Secretary-General or his designated representative. The Secretary-General shall ensure that only users authorized by him or her or other persons designated by him or shall have access to such data and information as are strictly necessary for a particular task. No duplication of these data and information shall be permitted, except as authorized by the Secretary-General for specific purposes, for example consideration by members of the Legal and Technical Commission or use by identified persons participating in a programme or activity of the Authority pursuant to the Convention or the Regulations. Where data and information are duplicated, the Secretary-General shall ensure that duplicated documents are numbered, distributed only on the basis of a log system, and are recovered and promptly destroyed after their usage.

**System Access Control**

5. The ICT resources used by the Secretariat for the storage, analysis and archiving of data and information covered by this annex shall aim to meet the criteria of a C2-level trusted system, (as described in Section 2.2 of the U.S. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC), DOD 5200.28-STD, December 1985). The following features are some of the ones provided by a C2-level trusted system:

(a) A stringent password and authentication system. Each user of the system is assigned a unique user identification and associated password. Each time the user logs on to the system he/she has to provide the correct password. Even when successfully logged on the user only has access to those and only to those functions and data that he/she is configured to have access to. Only a privileged user has access to all the data.

(b) Physical access to the computer system is controlled, including by compulsory biometric identification, video surveillance and a dual swipe card access system.

(c) Auditing; selective recording of events for analysis and detection of security breaches.

(d) Time-based access control; access to the system can be specified in terms of times-of-day and days-of-week that each user is allowed to login to the system.

(e) Terminal access control; specifying for each workstation which users are allowed to access.

**Authenticity and Data Access Security**

6. Data exchange protocols for electronic transmission of data and information covered by this annex between contractors or prospective contractors and the Secretariat shall be duly tested by the Secretariat.

**Communication Security**

7. Where necessary and appropriate, encryption protocols duly tested by the Secretariat shall be applied to ensure confidentiality and authenticity.

**Data Security**

8. Access limitation to the data and information shall be secured via a flexible user identification and password mechanism. Each user shall be given access only to the data necessary for his/her task.

**Security Procedures**

9. The Secretary-General shall nominate the IT Manager as the security system administrator. The security system administrator shall review the log files generated by the software, properly maintain the system security, restrict access to the system as deemed needed and act as a liaison with each contractor in order to solve security matters.

**Processing and handling of data and information**

10. All data and information submitted by contractors or prospective contractors (including applications for approval of plans of work for exploration) should be forwarded to the Office of the Secretary-General for proper handling and recording by staff specifically authorized for that purpose by the Secretary-General. Such handling and recording procedures shall include:

(a) The maintenance of a log and inventory system of all data, and information received by fax, electronic mail, air mail or courier, including its type and source and routing from the time of receipt until final disposition.

(b) Storage of confidential data and information in the Authority's vault at all times to prevent unauthorized access to, or removal of such data and information.

(c) Entry of relevant electronic data into a secure ICT resource as described in this annex.

11. Any member of staff who is authorized to having access to confidential data and information shall be required to sign a written declaration in the following format. A copy of such declaration shall be maintained on the individual's personnel file.

"DECLARATION OF CONFIDENTIALITY

I, the undersigned, hereby declare that I understand that, due to the nature of my work, I will handle and have access to confidential data and information in the form of applications, contracts, maps, reports, manuals, drawings, diagrams, correspondence, faxes, e-mail, data and computer programs, during the discharge of my duties at the Authority.

I acknowledge that I have a legal obligation under the Convention and the rules, regulations and procedures of the Authority with respect to the non-disclosure of confidential data and information.

I agree to comply with the applicable rules, regulations and procedures established to ensure the confidentiality of such data and information.

I shall not disclose, even after the termination of my functions with the Authority, any industrial secret, proprietary data, which are transferred to the Authority in accordance with Annex III, article 14, of the Convention, or any other confidential information coming to my knowledge by reason of my employment with the Authority.

Signature:
Name:
Department:
Date:
Name of Supervisor:
Signature:
Rank:
Date: …”