Secretariat

19 April 2017

Secretary-General's bulletin*

To: Members of the staff

From: The Secretary-General

Subject: **Acceptable use of communications and information technology resources and data**

With a view to implementing article 168 of the United Nations Convention on the Law of the Sea, the Secretary-General of the International Seabed Authority (ISA), for the purposes of defining the proper communications technology and related resources and data, and of ensuring the security and technical integrity of the system, promulgates the following:

Section 1
Definitions

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

(a) Authorized user: any staff member who is duly authorized to use communications and Information Technology (CIT) resources;

(b) Convention: 1982 United Nations Convention on the Law of the Sea;

(c) CIT resource: any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by the ISA;

(d) CIT data: any data or information, regardless of its form or medium, which is or has been electronically generated by, transmitted via, received by, processed by, or represented in an CIT resource and for official purposes;

(e) CIT Services: the Communications and Information Technology Services in the Office of Administrative Services;

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

(g) Personal use: use of CIT resources by an authorized user for other than official purposes and within the scope of his or her authorization;

(h) Sensitive data: CIT data that is classified or the use or distribution of which is otherwise restricted pursuant to applicable administrative issuances, **ISBA**/ST/SGB/2011/03.

* Issued without formal editing.

Section 2
Conditions applicable to the use of CIT resources and CIT data

2.1 Use of CIT resources and CIT data shall in all cases be in accordance with the provisions set out in this bulletin and such other administrative issuances as may apply to them.

2.2 Authorized uses shall promptly report to the appropriate officer, any violation of the provisions of this bulletin of which they become aware.

Section 3
Official use

3.1 Authorized users shall ensure that their use of CIT resources and CIT data is consistent with their obligations as staff members or such other obligations as may apply to them, as the case may be.

3.2 Authorized users shall use their best efforts:

(a) To ensure the accuracy of any CIT data for which they are responsible;

(b) To preserve and protect CIT resources and CIT data which may be needed by the organization for any official purpose;

(c) Access to, possession of, or distribution of sensitive data shall be in accordance with the applicable provisions of the Convention, the Staff Rules and Regulations, all rules, regulations and procedures of the ISA, administrative issuances applicable to such sensitive data, such as **ISBA**/ST/SGB/2011/03.

Section 4
Limited personal use

4.1 Authorized users shall be permitted limited personal use of CIT resources, provided such use:

(a) Is consistent with the highest standard of conduct for international civil servants (among the uses which would clearly not meet this standard are use of CIT resources for purposes of obtaining and distributing pornography, engaging in gambling, or downloading audio or video files to which a staff member is not legally entitled to have access);

(b) Would not reasonably be expected to compromise the interests or the reputation of the ISA;

(c) Involves minimal additional expenses to the Organization;

(d) Takes place during personal time or, if during working hours, does not significantly impinge on such working hours;

(e) Does not adversely affect the ability of the authorized user or any other authorized users to perform his or her official functions;

(f) Does not interfere with the activities and operations of the ISA or adversely affect the performance of CIT resources.

4.2 When making personal use of CIT resources, authorized users shall ensure that any such use clearly indicates that it is personal and not official in nature.

4.3 Personal use is a privilege that can be modified or revoked at any time, depending on the need of the ISA. Authorized users shall bear full responsibility and liability in connection with their personal use of CIT resources and the ISA shall not bear any responsibility or liability in respect thereof.

4.4 Paragraph 8 of **ISBA**/ST/SGB/2011/03, defines categories of records considered private papers of the staff members.

Section 5
Prohibited activities

5.1 Users of CIT resources and CIT data shall not engage in any of the following actions:

(a) Knowingly or through gross negligence, create false or misleading CIT data;

(b) Knowingly or through gross negligence, making CIT resources or CIT data available to persons who have not been authorized to access them;

(c) Knowingly or through gross negligence, using CIT resources or CIT data in a manner contrary to the rights and obligations of staff members;

(d) Knowingly and without justification and authorization, or through gross negligence, damaging, deleting, deteriorating, altering, extending, concealing or suppressing CIT resources or CIT data, including connecting or loading any non CIT resources or CIT data in violation of international copyright laws, patent, industrial secrets or any proprietary information;

(e) Knowingly accessing without authorization, CIT data of the whole or any part of a CIT resources, including electromagnetic transmissions;

(f) Knowingly or through gross negligence, using CIT resources and data in violation of the International Seabed Authority's contracts or other licensing agreements for use of such CIT resources or CIT data or in violation of international copyright laws, patent, industrial secrets or any proprietary information;

(g) Knowingly or through gross negligence, attempting, aiding or abetting the commission of any of the activities prohibited by this section.

Section 6
Rights in CIT resources; protection of technical integrity and performance of CIT resources

6.1 (a) The ISA shall retain all its rights in CIT resources and CIT data and in any official use, work product, including emails, audio and videos, of an authorized user using the ISA's CIT resources or CIT data; and

(b) The ISA shall have the rights to block or restrict access to any CIT resource or CIT data, at any time and without notice, when necessary for maintenance or restoring the technical integrity or performance thereof or for any other appropriate purpose, including prevention of any of the activities prohibited under section 5 of this bulletin.

Section 7
Monitoring and investigations

7.1 All use of CIT resources and CIT data shall be subject to monitoring and investigation as set forth in section 8 and section 9.

7.2 Monitoring and investigation shall be conducted only by the CIT Services, in accordance with the procedure set out in section 8 and section 9.

Section 8
Monitoring and investigation conducted by the CIT Services

8.1 Technical monitoring of the use of the CIT 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.

8.2 If at any time there is reason to believe that there has been use which interferes with the operation of CIT resources or technical disruption of CIT resources, the CIT Services may initiate monitoring or an investigation.

8.3 The CIT Services shall conduct an investigation upon request from any official authorized to initiate an investigation.

8.4 (a) Requests for investigation shall be addressed to the Secretary-General. Such requests must 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; and

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

8.5 The following procedures shall apply in cases of such investigations:

(a) Staff members and their supervisors shall be informed immediately preceding access to their CIT resources or CIT data, including electronic files, email and Intranet / Internet access records by the office recording the investigation;

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

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

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

(d) A special register must be maintained in a secure location in the CIT Services, 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;

(e) The data retrieved and provided to the requester shall not be retained by the CIT Services. The original signed written request and receipt for any data provided to the requesting office shall be kept in a separate file in the Executive Office of the Secretary-General and CIT User Manual; and

(f) Monitoring or investigation shall continue for only as 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 informed by the office that requested such monitoring or investigation.

Section 9
Commentaries

9.1 The commentaries contained in the annex to the present bulletin provide clarifications on the above sections.

9.2 Specific policies for various CIT facilities and services are described in the CIT User Manual issued to all staff and available from the CIT Services.

Section 10
Final Provision

10.1 The present bulletin shall enter into force on 19 April 2017.

Annex

Commentaries on various sections of the Acceptable Usage Policy

A. Commentary on section 1

1. This section provides definitions for key terms used throughout the bulletin.

2. **Definition (a)** covers all staff members who are authorized to use CIT resources. This would not include contractors, consultants, gratis personnel, interns, certain International Seabed Authority officials who are not staff members and other individuals affiliated with the ISA who are not staff members, but who are authorized to use CIT resources. Accordingly, the agreements or other documents governing the appointment of such individuals or entities should make the terms of this bulletin applicable to them, mutatis mutandis, whether by specific reference to this bulletin or other appropriate means. The authorization referred to in this definition and throughout the bulletin (except for **provision 4 (e)**) is that which can be reasonably construed to be granted under the user's official job responsibilities or by instructions from a superior whose official job responsibilities permit the giving of such instructions.

3. **Definition (c)** is intended to cover all hardware or software capable of handling or storing electronic data. Accordingly, it includes computer hardware (e.g., desktops, laptops, servers, printers), computer software (e.g., operating systems, productivity applications, database management systems), computer networks (e.g., physical media, switching equipment, firewalls, wireless facilities), telephone hardware, software and networks (e.g., wired PBX, cellular telephones), sound systems, voting systems, television and radio facilities, personal digital assistants, including those with wireless web and e-mail capabilities, security equipment (e.g., sensors, cameras, alarms, electronic access doors) and electronic building equipment (e.g., elevators, generators, heating, ventilation and air conditioning).

4. **Definition (d)** is intended broadly to cover all data or information that is created or received by the International Seabed Authority. It includes all data and information, regardless of its origin or the form it may subsequently take (e.g., telephone conversations, telephone logs, information transferred to a memo or other non-electronic medium from e-mail, word processing, fax, or other electronic media).

5. In **definition (f)**, “official functions” would include activities reasonably related to staff representation, such as the convocation of meetings, committees, and discussion of staff representation business.

6. In **definition (g),** the authorization referred to is that which is granted by **section 4** of this bulletin.

7. Together with the **definition** of “authorized user”, **definitions (f)** and **(g)** in section I create four categories of individuals:

(i) users who are not authorized users;

(ii) authorized users engaged in official use;

(iii) authorized users engaged in personal use;

(iv) authorized users engaged in use that is outside their scope of authorization.

8. **Definition (h)** is intended to cover CIT data which, for reasons of security, safety, privacy, confidentiality or other reasons, is classified or requires special protection, handling and awareness, in accordance with present and future administrative issuances. Regarding current issuances on information that is classified or the distribution of which is otherwise restricted, as stipulated in **ISBA**/ST/SGB/2011/03.

B. Commentary on section 2

1. In **provision 2.1 (a),** other administrative issuances which apply to CIT resources and CIT data include those cited above in reference to the definition of "sensitive data" in particular **ISBA**/ST/SGB/2011/03.

2. **Provision 2.2 (b)** imposes an obligation on staff members to report violations of the bulletin of which they become aware, even if the violation relates to CIT resources or CIT data that the staff member is not authorized to use or to which the staff member is not authorized to have access. Such a reporting obligation is consistent with obligations imposed by other administrative issuances, for example, regarding sexual exploitation and sexual abuse. However, this provision is intended to cover only violations of which staff members become aware in the normal course of their activities. In accordance with **provision 7.2** of this bulletin, staff members may not engage in investigations into the use of CIT resources or CIT data by other staff members without authorization. The appropriate authority to which violations should be reported may vary depending on the circumstances. Among the authorities to whom it may be appropriate to report violations would be a supervisor, the head of an office, or the Secretary-General.

C. Commentary on section 3

1. Authorized users are encouraged to make maximum use of CIT resources and CIT data, to the extent of their authorization to do so and with a view to performing their duties as effectively and efficiently as possible.

2. With regard to **provision 3.1**, authorized users are required to ensure that their use of CIT resources and CIT data are consistent with all other obligations relating thereto. In the case of staff members, this would include the Staff Regulations and Rules.

3. With regard to **provision 3.2**, as part of their obligations, authorized users must use their best efforts to make CIT data accessible to any other authorized user who requires such CIT data for the performance of the authorized user's official functions. The obligation to use best efforts to preserve and protect CIT resources and CIT data is especially important where they are required for purposes of conducting an investigation.

D. Commentary on section 4

1. This section recognizes that staff members may from time to time use CIT resources for personal purposes and allows limited use for such purposes subject to certain conditions.

2. **Provision 4.1 (a)** requires that an authorized user's personal use be consistent with the highest standard of conduct for international civil servants. This standard is elaborated in the Staff Regulations and Rules and the status, basic rights and duties of International Seabed Authority staff members.

3. In **provision 4.1 (c)**, minimal additional expense would include use of limited amounts of consumables, such as paper, ink, or toner, general wear and tear on equipment and nominal costs incurred with telecommunications traffic. Authorized users must not use the official default folder structure for their personal documents (*C:\users\username.isa\My Documents; C:\users\username.isa\My Picture's….*): Such folders are synchronized with various file servers, both locally and in the Cloud, with implemented usage quotas, and must host only official documents.

4. With regard to **provision 4.2**, in some cases, the nature or context of the use will clearly indicate that the use is personal and not official. In cases where the non-official nature of the use is not clear, the non-official nature of the use can be indicated, in the case of e-mail messages and other communications, by including the following disclaimer: "This communication is personal, and not official, in nature." The Office of Administrative Services may, in consultation with the Office of Legal Affairs, authorize alternative disclaimers for this purpose. Staff members should be careful to keep communications of a personal nature separate from those of an official nature.

5. With regard to **provision 4.3**, staff members should be aware that personal use of CIT resources, including any communications relating thereto, will not be considered official acts entitled to the ISA's privileges and immunities and that the ISA will cooperate with law enforcement authorities in addressing any personal use of an illegal nature.

E. Commentary on section 5

1. This section enumerates certain activities in which users of CIT resources and CIT data may not engage. In this regard, please see also paragraph 2 of the commentary to **section 4**.

2. Examples of activities prohibited under **provision 5.1 (a)** would include the creation of fraudulent documents, the modification of information so as to render it false and the forgery of electronic signatures.

3. An example of the activities prohibited under **provision 5.1 (b)** would be knowingly, or through gross negligence, revealing passwords to, or otherwise permitting the use by, unauthorized individuals of personal accounts to access CIT resources or CIT data.

4. The rights and obligations of staff members referred to in **provision 5.1 (c)** would include those elaborated in the Staff Regulations and Rules and the status, basic rights and duties of International Seabed Authority staff members.

5. An example of the activities prohibited under **provision 5.1 (e)** would be unauthorized scanning of CIT resources for security vulnerabilities or other purposes.

6. An example of the activities prohibited under **provision 5.1 (f)** would be knowingly, or through gross negligence, using pirated software, downloading audio or video files to which a staff member is not legally entitled to have access, or using software for which a valid license has not been obtained.

F. Commentary on sections 7, 8 and 9

1. **Sections 7, 8 and 9**, which govern monitoring and investigations involving CIT resources or CIT data, are premised on the principle that CIT resources or CIT data are the property of the ISA intended for official use and that any use of them by

staff members is subject to the rights of the ISA in such CIT resources or CIT data, including the right to access them without the knowledge or consent of the staff member.

2. **Section 8** sets forth procedures applicable to all monitoring and investigations.

3. **Provision 7.2** sets forth the officers which are authorized to conduct or assist in monitoring and investigations involving CIT resources or CIT data.

4. **Section 8** covers monitoring and investigations conducted by the CIT Services on its own authority or on behalf of other offices. The CIT Services may undertake monitoring and investigation on its own authority when there has been interference with or technical disruption of CIT resources or CIT data. They may also undertake to assist other offices in authorized investigations. Investigations involving CIT resources or CIT data shall be made, *inter alia*, where the requesting office determines that there is reason to believe that misconduct, including violations of the provisions of the present bulletin, have occurred. All investigations involving access to CIT resources or CIT data under section 8 (except those under **section 8.2**) require the prior approval of the Secretary-General.

5. **Provision 8.5** sets forth the specific procedures applicable to monitoring and investigations of staff members' use of CIT resources and CIT data and sets forth a number of rights of staff members who are the subject of monitoring or investigation, including the right to be notified in advance that CIT resources or CIT data used by them will be accessed.