OPCW **Conference of the States Parties**

Tenth Session
7 – 11 November 2005

C-10/DEC.9
10 November 2005
Original: ENGLISH

DECISION

AMENDMENTS TO THE OPCW POLICY ON CONFIDENTIALITY

The Conference of the States Parties,

Recalling its decision adopting the OPCW Policy on Confidentiality (OPOC) (C-I/DEC.13, dated 16 May 1997, and Corr.1, dated 20 March 2000);

Recalling also that, according to Part XI, paragraph 1, of the OPOC, any amendments to it proposed by the Director-General or any State Party shall be forwarded by the Director-General through the Executive Council (hereinafter "the Council") to the Conference for its consideration and approval in accordance with its Rules of Procedure;

Recalling further that in a particular instance the Council requested that the Commission for the Settlement of Disputes Related to Confidentiality (hereinafter "the Confidentiality Commission") review the OPOC and advise the Director-General on related procedures (agenda item 4 of EC-XVIII/2, dated 18 February 2000, and Corr.1, dated 3 March 2000);

Noting that at its Special Session the Confidentiality Commission made a number of recommendations regarding amendments to the OPOC (CC-V/I, dated 31 January 2001);

Noting also that, having agreed that the amendments to the OPOC drafted by the Technical Secretariat (hereinafter "the Secretariat") after the Special Session were consistent with the aforementioned recommendations, the Confidentiality Commission recommended that these amendments be forwarded by the Director-General, through the Council, to the Conference for consideration and approval (CC-V/2, dated 7 October 2003); and

Noting further the recommendation by the Council on this matter (EC-M-25/DEC.3, dated 9 November 2005);

Hereby:

Adopts the amendments to the OPOC annexed hereto.

Annex: Amendments to the OPCW Policy on Confidentiality

Annex

AMENDMENTS TO THE OPCW POLICY ON CONFIDENTIALITY[1]

	Reference	Previous Text	New Text
1.	Part VI, paragraph 1.2	These principles are to be applied in the detailed elaboration of all procedures relating to the handling of confidential information, including in the OPCW Inspection Manual, the Declaration Handbook, and the Information Management System (IMS). Further practical procedures shall be set out on the basis of these principles in administrative directives issued by the Director-General. The principles contained in this Part shall apply to all operations of the Organisation, within the Secretariat and other organs of the Organisation, as well as in their dealings with States Parties. States Parties which receive confidential information from the Organisation are required to protect it in accordance with obligations under paragraph 6 of Article VII and paragraph 4 of the Confidentiality Annex. States Parties should therefore establish or adapt suitable means of handling and protection for OPCW confidential information in a manner consistent with these principles.	These principles are to be applied in the detailed elaboration of all procedures relating to the handling of confidential information, including in the OPCW Inspection Manual, the Declaration Handbook, and the *Manual of Confidentiality Procedure (MCP)*. Further practical procedures shall be set out on the basis of these principles in administrative directives issued by the Director-General. The principles contained in this Part shall apply to all operations of the Organisation, within the Secretariat and other organs of the Organisation, as well as in their dealings with States Parties. States Parties which receive confidential information from the Organisation are required to protect it in accordance with obligations under paragraph 6 of Article VII and paragraph 4 of the Confidentiality Annex. States Parties should therefore establish or adapt suitable means of handling and protection for OPCW confidential information in a manner consistent with these principles.
2.	Part VI, paragraph 2.7	**ADMINISTRATION OF DISSEMINATION AND HANDLING PROCEDURES** An appropriate unit of the Secretariat[2] shall be charged with overall supervision of the administration of confidentiality provisions and the	*The Office of Confidentiality and Security (OCS) shall be charged by the Director-General with the overall supervision of the administration of confidentiality provisions. The Director-General may decide to delegate specific issues related to confidentiality to*

1 In the column entitled "New Text", changes appear in italics.

2 Confidentiality Annex, subparagraph 2(b).

	Reference	Previous Text	New Text
		Director-General may specifically authorise the head of this unit to exercise certain delegations of the authority relating to confidentiality. The precise identity of this unit will be determined through general planning of the Secretariat, but for the purposes of this document it is referred to as the "designated confidentiality unit".[3]	*the Head of the OCS. Ultimate responsibility for confidentiality remains with the Director-General.*
3.	Part VI paragraph 2.8	The designated confidentiality unit will supervise the routine operation of these handling procedures.	The *OCS* will supervise the routine operation of these handling procedures.
4.	Part VI paragraph 3.3	When information is received by the Organisation from any of these sources, specific obligations are incurred to protect and handle it appropriately. In particular, the initial recipient or the originator of the information is obliged to ensure that the confidentiality content is clearly determined, and that the correct classification has been applied, in consultation where necessary with the designated confidentiality unit. Confidential information which is compiled or synthesised by Secretariat staff members, and which draws on confidential information originating from States Parties shall, as a rule, bear at a minimum the classification designated by the State Party, unless the level of the sensitivity of the information has been reduced with the consent of the originating State Party, or the level of sensitivity is determined to be higher. Any deviation from this rule shall be confirmed by the	When information is received by the Organisation from any of these sources, specific obligations are incurred to protect and handle it appropriately. In particular, the initial recipient or the originator of the information is obliged to ensure that the confidentiality content is clearly determined, and that the correct classification has been applied, in consultation where necessary with the *OCS*. Confidential information which is compiled or synthesised by Secretariat staff members, and which draws on confidential information originating from States Parties shall, as a rule, bear at a minimum the classification designated by the State Party, unless the level of the sensitivity of the information has been reduced with the consent of the originating State Party, or the level of sensitivity is determined to be higher. Any deviation from this rule shall be *authorised by the Director-General or by a member*

3 If and when a decision is reached, in the course of planning the OPCW Technical Secretariat structure, on the specific identity of this unit, its name will be substituted accordingly here and throughout this Policy.

	Reference	Previous Text	New Text
		Director-General's delegate in the designated confidentiality unit.	*of staff authorised by him to do so. The Director-General has authorised the Head of OCS to do so.*
5.	Part VI paragraph 3.9(b)	(b) persons, who are not permanent staff members, to whom access has been granted under the provisions of subparagraphs 2.12 and 2.13 of this Part, such as authorised experts or authorised personnel of a designated laboratory who are individually bound by secrecy agreements; in such a case the amount of information disclosed shall be kept to a minimum, yet should be sufficient to facilitate the task for which the access was granted; and	(b) persons *who are not staff members and* to whom access has been granted under the provisions of subparagraphs 2.12 and 2.13 of this Part, such as authorised experts or authorised personnel of a designated laboratory who are individually bound by secrecy agreements; in such a case the amount of information disclosed shall be kept to a minimum *and any such information shall be provided on a need-to-know basis*, yet should be sufficient to facilitate the task for which the access was granted; and
6.	Part VI paragraph 3.10	The Director-General shall issue and the designated confidentiality unit shall supervise the implementation of administrative directives setting out detailed practical handling procedures for the following categories of physical media, to ensure the protection of confidential information each such medium carries during all handling and storage operations:	The Director-General shall issue, and the *OCS* shall supervise the implementation of administrative directives setting out detailed practical handling procedures for the following categories of physical media, to ensure the protection of confidential information each such medium carries during all handling and storage operations:
7.	Part VI, paragraph 4.1	**Marking of confidential information** In order to ensure the proper handling of OPCW confidential information, all documents and media for information storage shall be clearly marked in accordance with the marking instructions set out in an administrative directive issued by the Director-General and supervised by the designated confidentiality unit.	**Marking of confidential information** In order to ensure the proper handling of OPCW confidential information, all documents and media for information storage shall be clearly marked in accordance with the marking instructions set out in an administrative directive issued by the Director-General and supervised by the *OCS*.

	Reference	Previous Text	New Text
8.	Part VI, paragraph 4.2	Each individual document must be clearly marked according to the highest level of sensitivity of the material it contains. Where this may facilitate subsequent release or dissemination of less sensitive portions of a document, the principle of portion marking may be applied so that classification indications are given of the particular levels of sensitivity of sections within a document, the overall document being clearly marked as bearing the highest level of sensitivity.	Each individual document must be clearly marked according to the highest level of sensitivity of the material it contains. Where this may facilitate subsequent release or dissemination of less sensitive portions of a document, the principle of portion *(paragraph)* marking may be applied so that classification indications are given of the particular levels of sensitivity of sections within a document, the overall document being clearly marked as bearing the highest level of sensitivity. *Alternatively, all confidential information may be contained in a confidential annex to an otherwise unclassified document, the overall document to be clearly marked as bearing the highest level of sensitivity.*
9.	Part VI paragraph 4.3	The Confidentiality Annex stipulates that all data and documents obtained by the Secretariat shall first be evaluated for confidentiality content (subparagraph 2(b)) and that, if confidential, such data and documents shall then be classified (subparagraph 2(d)); this process shall accord with the right of any State Party to designate information it provides as confidential. The designated confidentiality unit will be the appropriate unit for this task, and will therefore implement procedures to ensure that all information with possible confidentiality content which has been acquired from outside the Secretariat is evaluated and any necessary classification is clearly marked.	The Confidentiality Annex stipulates that all data and documents obtained by the Secretariat shall first be evaluated for confidentiality content (subparagraph 2(b)) and that, if confidential, such data and documents shall then be classified (subparagraph 2(d)); this process shall accord with the right of any State Party to designate information it provides as confidential. *The unit of the Secretariat that receives a given document will be the appropriate unit for this task and, when it deems it necessary, will therefore implement procedures, with the assistance of the OCS,* to ensure that all information with possible confidentiality content which has been acquired from outside the Secretariat is evaluated and any necessary classification is clearly marked.

	Reference	Previous Text	New Text
10.	Part VI paragraph 4.4	All confidential information generated in the Secretariat is required to be clearly marked by its originator in accordance with a provisional classification category relevant to its sensitivity. The level of this classification must be determined in accordance with the OPCW Classification System. Branch heads must supervise the proper marking of internally generated confidential material, under the overall coordination and authority of the designated confidentiality unit.	All confidential information generated in the Secretariat is required to be clearly marked by its originator in accordance with a provisional classification category relevant to its sensitivity. The level of this classification must be determined in accordance with the OPCW Classification System. Branch heads must supervise the proper marking of internally generated confidential material, under the overall coordination and authority of the *OCS*.
11.	Part VI paragraph 4.6	**Filing and record-keeping** Filing and record-keeping procedures to ensure that the internal routing and filing of confidential information are registered shall be established by the Secretariat in accordance with an administrative directive issued by the Director-General and supervised by the designated confidentiality unit. These procedures shall record the provision of any such confidential information to any individual, agency or body within and beyond the Secretariat, including to representatives of States Parties.	**Filing and record-keeping** Filing and record-keeping procedures to ensure that the internal routing and filing of confidential information are registered shall be established by the Secretariat in accordance with an administrative directive issued by the Director-General and supervised by the *OCS*. These procedures shall record the provision of any such confidential information to any individual, agency or body within and beyond the Secretariat, including to representatives of States Parties.
12.	Part VI paragraph 4.9	**OPCW HIGHLY PROTECTED** information can be copied only after obtaining the registered consent of an authorised senior staff member other than the staff member who will be copying the information, or in terms of a specific standing order. Such consent may specify that the copying must be done under the supervision of another staff member. The number of copies taken must be recorded, and each copy numbered. Copies should	*Classified information shall be copied only under disciplined and auditable conditions.* **OPCW HIGHLY PROTECTED** information can be copied only after obtaining the registered consent of an authorised senior staff member other than the staff member who will be copying the information, or in terms of a specific standing order. Such consent may specify that the copying must be done under the supervision of another staff

	Reference	Previous Text	New Text
		be distributed to any approved recipients, with this transmission recorded. Any surplus copies, or copies no longer in use shall be returned to the filing clerk, who shall either file or destroy them, recording this action.	member. The number of copies taken must be recorded, and each copy numbered. Copies should be distributed to any approved recipients, with this transmission recorded. Any surplus copies, or copies no longer in use shall be returned to the filing clerk, who shall either file or destroy them, recording this action.
13.	Part VI paragraph 4.15	**Safeguarding of confidential information** Staff members and other authorised personnel using confidential information or who are responsible for its safe-keeping must take every precaution to prevent deliberate or accidental access to such information by unauthorised persons.	**Safeguarding of confidential information** Staff *members*, and other *personnel authorised in accordance with paragraphs 2.12 and 2.13 above, who are using confidential information or are* responsible for its safe-keeping must take every precaution to prevent deliberate or accidental access to such information by unauthorised persons.
14.	Part VI paragraph 4.16	Confidential information must not be used or placed so that it is exposed or made accessible to individuals not authorised to have access to such information. The designated confidentiality unit shall establish procedures to ensure that confidential information is properly handled by Secretariat staff members, and the Director-General shall ensure that these procedures are fully carried out, that any violations are detected and reported, and that appropriate disciplinary sanctions are imposed in accordance with Part IX of this Policy**.**	Confidential information must not be used or placed so that it is exposed or made accessible to individuals not authorised to have access to such information. *The Director-General has designated the OCS to establish procedures to ensure that confidential information is properly handled by Secretariat staff members*, and the Director-General shall ensure that these procedures are fully carried out, that any violations are detected and reported, and that appropriate disciplinary sanctions are imposed in accordance with Part IX of this Policy.

	Reference	Previous Text	New Text
15.	Part VI paragraph 5.3	**Confidential information in computers and computer material** Access to all sites of the OPCW and key components of the IMS, such as the servers and mass storage devices, must be controlled. All hardware of the IMS and especially workstations, servers and user terminals shall be protected, not only from theft or criminal damage, but also from unauthorised physical access and tampering attempts. In addition, maintenance and repair activities on IMS hardware shall be supervised and recorded. Access to such hardware items as servers, printers, back-up devices, as well as other output devices, shall be limited to staff members with appropriate clearances.	**Confidential information in computers and computer material** Access to all sites of the OPCW and key components of the IMS, such as the servers and mass storage devices, must be controlled. All hardware *in the confidential part of* the IMS, and especially workstations, servers, printers, and user terminals shall be protected, not only from theft or criminal damage, but also from unauthorised physical access and tampering attempts. In addition, maintenance and repair activities on *confidential* IMS hardware shall be supervised and recorded. Access to such hardware items as servers, printers, back-up devices, as well as other output devices, shall be limited to staff members with appropriate clearances.
16.	Part VI paragraph 5.4	Procedures for the protection of confidential data stored within the IMS and any other electronic data-processing system or storage device shall incorporate the following elements: - access control measures against unauthorised users or any unauthorised external access; - separation of the files and data of the various users; and - audit on user activities including access to the databases and changes made to operating system parameters and system files. In particular, any access by individual staff to computer files containing confidential information shall be recorded and regular audits conducted of these records.	*Procedures for the protection of data stored within the confidential part of the IMS* and any other electronic data-processing system or storage device shall incorporate the following elements: - access control measures against unauthorised users or any unauthorised external access; - separation of the files and data of the various users; and - audit on user activities including access to the databases and changes made to operating system parameters and system files. In particular, any access by individual staff to computer files containing confidential information shall be recorded and regular audits conducted of these records.

	Reference	Previous Text	New Text
17.	Part VIII, paragraph 3	**Administration of the confidentiality regime in the Secretariat** The confidentiality regime shall apply to the operations of all elements of the Secretariat. An appropriate unit of the Secretariat shall be designated for the task of evaluating all data and documents obtained by the Secretariat, to establish whether they contain confidential information, applying the guidelines set out in subparagraph 2(a) of the Confidentiality Annex and paragraph 11 of Part III of this Policy. Auditing of the operation of the confidentiality regime shall be conducted internally by the Secretariat and shall be kept functionally distinct from any unit tasked with its implementation.	**Administration of the confidentiality regime in the Secretariat** The confidentiality regime shall apply to the operations of all elements of the Secretariat. *The OCS shall assist the receiving Secretariat units in reviewing* data and documents obtained by the Secretariat, to establish whether they contain confidential information, applying the guidelines set out in subparagraph 2(a) of the Confidentiality Annex and paragraph 11 of Part III of this Policy. Auditing of the operation of the confidentiality regime shall be conducted by *the Office of Internal Oversight in the exercise of its confidentiality-audit function,* and shall be kept functionally distinct from any unit tasked with its implementation.
18.	Part VIII, paragraph 4	Under the Director-General's supervision, the Secretariat shall ensure that its staff members are properly advised and reminded about their obligation to protect confidential information and to abide by the confidentiality regime, as well as about the principles of this Policy and the procedures required to implement it, the principles and procedures relating to security, and the possible penalties that they would incur in the event of unauthorised disclosure of confidential information.	Under the Director-General's supervision, the Secretariat shall ensure that its staff members are properly advised and reminded about their obligation to protect confidential information and to abide by the confidentiality regime, as well as about the principles of this Policy and the procedures required to implement it, the principles and procedures relating to security, and the possible penalties that they would incur in the event of unauthorised disclosure of confidential information. *Training requirements shall also be taken into account following any change in the organisational structure of the Secretariat that affects personnel handling confidential material. In such cases, these additional training requirements shall be met preferably within three months, but*

	Reference	Previous Text	New Text
			in any event as soon as possible after the introduction of the structural change in question.
19.	Part IX.1 paragraph 3.4	When a decision has been taken to proceed with an investigation, the decision should be made known immediately to any States Parties and any Secretariat staff member involved in the alleged breach or suspected violation.	When a decision has been taken *by the Director-General* to proceed with an investigation, the decision should be made known immediately to any States Parties and any Secretariat staff member involved in the alleged breach or suspected violation.
20.	Part IX.1 paragraph 3.6	The Director-General shall be directly responsible for the investigation, and will direct it personally, but may appoint a designated senior staff member to conduct investigatory work.	The Director-General shall be directly responsible for the investigation, and will direct it personally, but may *designate* a senior staff member to conduct investigatory work.
21.	Part IX.1 paragraph 7.1	If, on conclusion of the investigation, it is determined that a breach or violation has been committed by a serving Secretariat staff member, the Director-General shall apply proper disciplinary measures in accordance with the OPCW Staff Regulations and Rules.	If, on conclusion of the investigation, it is determined that a breach or violation has been committed *by a Secretariat staff member*, the Director-General shall apply proper disciplinary measures in accordance with the OPCW Staff Regulations and Rules.
22.	Part IX.1 paragraph 8	**Step 4b: Sanctions against former Secretariat staff** If a breach or violation is determined within the report to have been committed by a former member of staff of the Secretariat, the Director-General may decide on the application of whatever measures may still be applied within the terms of the OPCW Staff Regulations and Rules. This may include the loss of pension rights acquired during service with the Organisation or the cancellation of residual financial or other entitlements.	**Step 4b: Sanctions against former Secretariat staff** If a breach or violation is determined within the report to have been committed by a former member of staff of the Secretariat, the Director-General may decide on the application of whatever measures may still be applied within the terms of the OPCW Staff Regulations and Rules. *This may include the loss of financial or other entitlements, such as those related to the OPCW Provident Fund.*

	Reference	Previous Text	New Text
23.	Part IX.2 paragraph 3	**Rules governing the operating procedures of the Confidentiality Commission** These rules govern the detailed operating Procedures for the Confidentiality Commission, which are to be approved by the Conference.	**Rules governing the operating procedures of the Confidentiality Commission** *These rules were approved by the Third Session of the Conference and govern the detailed operating Procedures for the Confidentiality Commission.*
24.	Part XI paragraph 2	The Director-General shall, without delay, issue any changes to administrative directives that are made necessary by the Conference's approval of amendments to this Policy, and shall report on any such changes to the Executive Council and to the Conference in the annual report on the confidentiality regime.	The Director-General shall, without delay, issue any changes to administrative directives that are made necessary by the Conference's approval of amendments to this Policy, and shall report on any such changes to the Executive Council and to the Conference in the annual report on the confidentiality regime. *The Director-General shall ensure that all staff employed by the Organisation are informed of such changes immediately and receive related training, preferably within three months, but in any event as soon as possible after their introduction.*
25.	Glossary		*MCP: Manual of Confidentiality Procedure* *OCS: Office of Confidentiality and Security in the Technical Secretariat* *IMS: Information Management System*

- - - o - - -