

# **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<sup>1</sup>

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

<sup>1</sup> In the column entitled "New Text", changes appear in italics.

<sup>2</sup> Confidentiality Annex, subparagraph 2(b).

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

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

	Reference	Previous Text	New Text
10.	Part VI	All confidential information	All confidential information
	paragraph 4.4	generated in the Secretariat is	generated in the Secretariat is
		required to be clearly marked by	required to be clearly marked by its
		its originator in accordance with a	originator in accordance with a
		provisional classification category	provisional classification category
		relevant to its sensitivity. The	relevant to its sensitivity. The level
		level of this classification must be	of this classification must be
		determined in accordance with	determined in accordance with the
		the OPCW Classification System.	OPCW Classification System.
		Branch heads must supervise the	Branch heads must supervise the
		proper marking of internally	proper marking of internally
		generated confidential material,	generated confidential material,
		under the overall coordination	under the overall coordination and
		and authority of the designated	authority of the OCS.
		confidentiality unit.	
11.	Part VI	Filing and record-keeping	Filing and record-keeping
	paragraph 4.6	Filing and record-keeping	Filing and record-keeping
		procedures to ensure that the	procedures to ensure that the
		internal routing and filing of	internal routing and filing of
		confidential information are	confidential information are
		registered shall be established by	registered shall be established by
		the Secretariat in accordance with	the Secretariat in accordance with
		an administrative directive issued	an administrative directive issued
		by the Director-General and	by the Director-General and
		supervised by the designated	supervised by the OCS. These
		confidentiality unit. These	procedures shall record the
		procedures shall record the	provision of any such confidential
		provision of any such confidential information to any individual,	information to any individual,
		agency or body within and	agency or body within and beyond the Secretariat, including to
		beyond the Secretariat, including	
		to representatives of States	representatives of States Parties.
		Parties.	
12.	Part VI	OPCW HIGHLY PROTECTED	Classified information shall be
12.	paragraph 4.9	information can be copied only	copied only under disciplined and
	paragraph 4.7	after obtaining the registered	auditable conditions. <b>OPCW</b>
		consent of an authorised senior	HIGHLY PROTECTED
		staff member other than the staff	information can be copied only
		member who will be copying the	after obtaining the registered
		information, or in terms of a	consent of an authorised senior
		specific standing order. Such	staff member other than the staff
		consent may specify that the	member who will be copying the
		copying must be done under the	information, or in terms of a
		supervision of another staff	specific standing order. Such
		member. The number of copies	consent may specify that the
		taken must be recorded, and each	copying must be done under the
		copy numbered. Copies should	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	Safeguarding of confidential	Safeguarding of confidential
	paragraph 4.15	information	<b>information</b> Staff <i>members</i> , and
		Staff members and other	other personnel authorised in
		authorised personnel using	accordance with paragraphs 2.12
		confidential information or who	and 2.13 above, who are using
		are responsible for its safe-	confidential information or are
		keeping must take every	responsible for its safe-keeping
		precaution to prevent deliberate or accidental access to such	must take every precaution to prevent deliberate or accidental
		information by unauthorised	access to such information by
		persons.	unauthorised persons.
14.	Part VI	Confidential information must not	Confidential information must not
1	paragraph 4.16	be used or placed so that it is	be used or placed so that it is
		exposed or made accessible to	exposed or made accessible to
		individuals not authorised to have	individuals not authorised to have
		access to such information. The	access to such information. The
		designated confidentiality unit	Director-General has designated
		shall establish procedures to	the OCS to establish procedures to
		ensure that confidential	ensure that confidential
		information is properly handled	information is properly handled by
		by Secretariat staff members, and	Secretariat staff members, and the
		the Director-General shall ensure	Director-General shall ensure that
		that these procedures are fully	these procedures are fully carried
		carried out, that any violations are	out, that any violations are detected
		detected and reported, and that	and reported, and that appropriate
		appropriate disciplinary sanctions are imposed in accordance with	disciplinary sanctions are imposed in accordance with Part IX of this
		_	
		Part IX of this Policy.	Policy.

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

	Reference	Previous Text	New Text
17.	Part VIII,	Administration of the	Administration of the
	paragraph 3	confidentiality regime in the	confidentiality regime in the
		Secretariat	Secretariat
		The confidentiality regime shall	The confidentiality regime shall
		apply to the operations of all	apply to the operations of all
		elements of the Secretariat. An	elements of the Secretariat. The
		appropriate unit of the Secretariat	OCS shall assist the receiving
		shall be designated for the task of	Secretariat units in reviewing data
		evaluating all data and documents	and documents obtained by the
		obtained by the Secretariat, to	Secretariat, to establish whether
		establish whether they contain	they contain confidential
		confidential information,	information, applying the
		applying the guidelines set out in	guidelines set out in subparagraph
		subparagraph 2(a) of the	2(a) of the Confidentiality Annex
		Confidentiality Annex and	and paragraph 11 of Part III of this
		paragraph 11 of Part III of this	Policy. Auditing of the operation
		Policy. Auditing of the operation	of the confidentiality regime shall
		of the confidentiality regime shall	be conducted by the Office of
		be conducted internally by the	Internal Oversight in the exercise of
		Secretariat and shall be kept	its confidentiality-audit function,
		functionally distinct from any unit	and shall be kept functionally
		tasked with its implementation.	distinct from any unit tasked with
L			its implementation.
18.	,	Under the Director-General's	Under the Director-General's
	paragraph 4	supervision, the Secretariat shall	supervision, the Secretariat shall
		ensure that its staff members are	ensure that its staff members are
		properly advised and reminded	properly advised and reminded
		about their obligation to protect confidential information and to	about their obligation to protect confidential information and to
			abide by the confidentiality regime,
		abide by the confidentiality regime, as well as about the	as well as about the principles of
		principles of this Policy and the	this Policy and the procedures
		procedures required to implement	required to implement it, the
		it, the principles and procedures	principles and procedures relating
		relating to security, and the	to security, and the possible
		possible penalties that they would	penalties that they would incur in
		incur in the event of unauthorised	the event of unauthorised disclosure
		disclosure of confidential	of confidential information.
		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	When a decision has been taken	When a decision has been taken by
	paragraph 3.4	to proceed with an investigation,	the Director-General to proceed
		the decision should be made	with an investigation, the decision
		known immediately to any States	should be made known
		Parties and any Secretariat staff	immediately to any States Parties
		member involved in the alleged	and any Secretariat staff member
		breach or suspected violation.	involved in the alleged breach or
			suspected violation.
20.	Part IX.1	The Director-General shall be	The Director-General shall be
	paragraph 3.6	directly responsible for the	directly responsible for the
		investigation, and will direct it	investigation, and will direct it
		personally, but may appoint a	personally, but may <i>designate</i> a
		designated senior staff member to	senior staff member to conduct
		conduct investigatory work.	investigatory work.
21.		If, on conclusion of the	If, on conclusion of the
	paragraph 7.1	investigation, it is determined that	investigation, it is determined that a
		a breach or violation has been	breach or violation has been
		committed by a serving	committed by a Secretariat staff
		Secretariat staff member, the	<i>member</i> , the Director-General shall
		Director-General shall apply	apply proper disciplinary measures
		proper disciplinary measures in	in accordance with the OPCW Staff
		accordance with the OPCW Staff	Regulations and Rules.
		Regulations and Rules.	
22.		Step 4b: Sanctions against	Step 4b: Sanctions against
	paragraph 8	former Secretariat staff	former Secretariat staff
		If a breach or violation is	If a breach or violation is
		determined within the report to	determined within the report to
		have been committed by a former	have been committed by a former
		member of staff of the Secretariat,	member of staff of the Secretariat,
		the Director-General may decide	the Director-General may decide on
		on the application of whatever	the application of whatever
		measures may still be applied	measures may still be applied
		within the terms of the OPCW	within the terms of the OPCW Staff
		Staff Regulations and Rules. This	Regulations and Rules. This may
		may include the loss of pension	include the loss of financial or
		rights acquired during service	other entitlements, such as those related to the OPCW Provident
		with the Organisation or the cancellation of residual financial	Fund.
			r una.
		or other entitlements.	

	Reference	Previous Text	New Text
23.	Part IX.2	Rules governing the operating	Rules governing the operating
	paragraph 3	procedures of the	procedures of the Confidentiality
		Confidentiality Commission	Commission
		These rules govern the detailed	These rules were approved by the
		operating Procedures for the	Third Session of the Conference
		Confidentiality Commission,	and govern the detailed operating
		which are to be approved by the	Procedures for the Confidentiality
		Conference.	Commission.
24.	Part XI	The Director-General shall,	The Director-General shall, without
	paragraph 2	without delay, issue any changes	delay, issue any changes to
		to administrative directives that	administrative directives that are
		are made necessary by the	made necessary by the
		Conference's approval of	Conference's approval of
		amendments to this Policy, and	amendments to this Policy, and
		shall report on any such changes	shall report on any such changes to
		to the Executive Council and to	the Executive Council and to the
		the Conference in the annual	Conference in the annual report on
		report on the confidentiality	the confidentiality regime. <i>The</i>
		regime.	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