OPCW **Conference of the States Parties**

Twenty-Second Session
27 November – 1 December 2017

C-I/DEC.13/Rev.2
30 November 2017
Original: ENGLISH

DECISION[1]

- **GUIDELINES FOR PROCEDURES ON THE RELEASE OF CLASSIFIED INFORMATION BY THE OPCW, IN ACCORDANCE WITH SUBPARAGRAPH 2(C)(III) OF THE CONFIDENTIALITY ANNEX**

- **A CLASSIFICATION SYSTEM FOR LEVELS OF SENSITIVITY OF CONFIDENTIAL DATA AND DOCUMENTS, TAKING INTO ACCOUNT RELEVANT WORK UNDERTAKEN IN THE PREPARATION OF THE CONVENTION, IN ACCORDANCE WITH SUBPARAGRAPH 2(D) OF THE CONFIDENTIALITY ANNEX**

- **RECOMMENDATIONS FOR PROCEDURES TO BE FOLLOWED IN CASE OF BREACHES OR ALLEGED BREACHES OF CONFIDENTIALITY, IN ACCORDANCE WITH PARAGRAPH 18 OF THE CONFIDENTIALITY ANNEX (PARIS RESOLUTION, SUBPARAGRAPHS 12(U), (V), AND (W))**

The Conference of the States Parties,

Recalling that the Preparatory Commission developed a draft OPCW Policy on Confidentiality (OPOC) that includes the above-mentioned issues as well as rules governing the composition and operating procedures of the Commission for the Settlement of Disputes Related to Confidentiality (hereinafter "the Confidentiality Commission") as required by paragraph 23 of the Confidentiality Annex to the Chemical Weapons Convention (hereinafter "the Confidentiality Annex"), in a combined manner;

Recalling also that the Preparatory Commission adopted the draft OPOC, as annexed to PC-XI/B/WP.8, dated 23 June 1995, and as amended by Working Group B, and decided to apply the provisions of this draft OPOC, *mutatis mutandis*, to the work of the Preparatory Commission (paragraph 7.7 of PC-XI/17, dated 27 July 1995; Corr.1, dated 14 August 1995; and Corr.2, dated 12 September 1995);

---

[1] The revised version of the OPCW Policy on Confidentiality (OPOC) annexed hereto contains three sets of changes—those that were made in C-I/DEC.13/Corr.1, dated 20 March 2000, which removed references to the draft OPOC submitted by the Preparatory Commission; those from C-10/DEC.9, dated 10 November 2005, which contains amendments to the OPOC; and those that were approved by the Conference of the States Parties at its Twenty-Second Session (C-22/DEC.15, dated 30 November 2017). The paragraph numbering in the revised version has been adjusted without changing the order of the content.

Recalling further that the Preparatory Commission decided to correct the clerical error in the second-to-last line of paragraph 6.2 of Part VI of the draft OPOC by replacing the word "should" with "shall"(paragraph 8.7 of PC-XII/17, dated 14 December 1995); and

Bearing in mind that the Preparatory Commission recommended, in paragraph 45.4 of its final report (PC-XVI/37, dated 15 April 1997), that the Conference of the States Parties (hereinafter "the Conference") adopt the above-mentioned OPOC, as amended;

Hereby:

Adopts the above-mentioned OPOC, which is annexed hereto, as amended.

Annex: OPCW Policy on Confidentiality

Annex

THE ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS

OPCW POLICY ON CONFIDENTIALITY

The Hague

MAY 1997

CONTENTS

OPCW Policy on Confidentiality[2]

[2] The original version of the OPOC was prefaced by the following note:

> "The Draft OPCW Policy on Confidentiality was developed by the Expert Group on Confidentiality (Annex to PC-XI/B/WP.8) and was adopted as amended by the Preparatory Commission at its Eleventh Session (PC-XI/17, paragraph 7.7 and PC-XI/B/12, paragraph 7.2). The Draft OPCW Media and Public Affairs Policy was developed by the Formal Consultations on OPCW Media and Public Affairs Policy (Attachment to PC-X/A/WP.5) and was provisionally approved as amended by the Preparatory Commission at its Tenth Session (PC-X/23, paragraph 6.11 and PC-X/A/3, paragraph 6.4), pending the adoption of other relevant documents including the Draft OPCW Policy on Confidentiality.
>
> The Preparatory Commission also decided that the Draft OPCW Policy on Confidentiality and the Draft OPCW Media and Public Affairs Policy would apply, *mutatis mutandis*, to the work of the Preparatory Commission (PC-XI/17, paragraph 7.7 and PC-X/23, paragraph 6.12 respectively).
>
> Ian R. Kenyon
> Executive Secretary"

(blank page)

PART I

INTRODUCTION

1. This document sets out the Organisation's policy for protecting confidentiality throughout activities related to the implementation of the Convention, for classifying and handling confidential information, and for dealing with breaches of confidentiality.

2. A policy for confidential information is essential to the work of the Organisation because of the intrusive verification measures which are aimed at promoting confidence in compliance with the Convention while respecting States Parties' legitimate concerns about the possible disclosure of sensitive information. Credible verification entails receptiveness on the part of States Parties and a level of intrusiveness in verification activities. The need for disclosure of appropriate information to demonstrate compliance with the Convention should be matched by credible reassurances for States Parties that proper measures are taken to prevent disclosure of information not relevant to the Convention and that any confidential information, once disclosed, will be appropriately protected.

3. Consequently, in defining States Parties' rights and obligations, the Convention embodies a balance between that disclosure necessary to enhance confidence in compliance with the Convention, and the prevention of disclosure of information not relevant to the Convention, in order to protect national security and proprietary rights, taking into account constitutional obligations. These two objectives are not necessarily in conflict; on the contrary, a credible and effective process of verification can be achieved which actively and integrally protects confidentiality. The Convention text provides practical assurances that all confidential information will be appropriately protected; and that verification procedures will seek to prevent the disclosure of information not related to verification of compliance with the Convention.

PART II

GENERAL POLICY

1. Paragraph 5 of Article VIII of the Convention provides the basis of the obligations of the Organisation to respect confidentiality:

   "The Organisation shall conduct its verification activities provided for under this Convention in the least intrusive manner possible consistent with the timely and efficient accomplishment of their objectives. It shall request only information and data necessary to fulfil its responsibilities under this Convention. It shall take every precaution to protect the confidentiality of information on civil and military activities and facilities coming to its knowledge in the implementation of this Convention and, in particular, shall abide by the provisions set forth in the Confidentiality Annex."

2. Paragraph 6 of Article VII of the Convention establishes the obligation on each State Party to:

   "treat as confidential and afford special handling to information and data that it receives in confidence from the Organisation in connection with the implementation of this Convention. It shall treat such information and data exclusively in connection with its rights and obligations under this Convention and in accordance with the provisions set forth in the Confidentiality Annex."

3. These basic requirements are elaborated in a number of other provisions of the Convention, especially in the Confidentiality Annex and in the provisions detailing verification procedures (e.g. paragraph 10 of Article VI; paragraphs 56 and 62, Part II of the Verification Annex and paragraph 48, Part X of the Verification Annex). From this basis, the fundamental elements of the OPOC are:

   (a) only that information necessary for the timely and efficient carrying out of its responsibilities under the Convention shall be sought and required; and requirements for information to which the Organisation shall be given access by a State Party shall be specified as precisely as possible;

   (b) verification activities shall be designed, planned and carried out so as to avoid unnecessary disclosure of confidential information and so as to seek to prevent disclosure of such information not related to compliance with the Convention, consistent with effective and timely discharge of verification obligations under the Convention;

   (c) confidential information not relevant to the Convention shall not be sought, recorded or retained in the course of verification or other activities, without prejudice to a State Party's right to request such a disclosure in accordance with the Convention. Once disclosed, it shall be protected, shall not be further disseminated, and shall be appropriately disposed of;

(d) systematic procedures for limiting the dissemination of and access to information after it is collected and classified as confidential shall be established, monitored, and adhered to;

(e) information obtained in connection with the implementation of the Convention shall not be published or otherwise released unless with explicit authority and in accordance with the release procedures outlined in Part VII of this policy; and

(f) staff selection and training, and staffing policy and regulations, shall take into account the need to ensure that all staff members, consultants and other contracted personnel, (hereinafter referred to as “staff members” or “employees”) of the Secretariat meet the highest standards of efficiency, competence and integrity.

PART III

INFORMATION AND CONFIDENTIALITY

1. Introduction

1.1 This Part sets out guidelines for developing a practical understanding of the scope of the terms 'information', 'confidential information' and 'confidentiality'. The Convention sets out no definitive account of how these terms are to be applied, and it is clear that they are to be determined in an operational context consistent with the implementation of the Organisation's and States Parties' various responsibilities under the Convention.

1.2 The Organisation will carry out its responsibilities greatly depending on the information obtained through its verification activities and provided by States Parties. Thus, information will be coming into the Organisation's possession or to a staff member of the Organisation in a continuous input-output pattern of acquiring, processing and producing further necessary information.

1.3 In view of the integral role of confidentiality in all the Organisation's activities, information can generally be considered in operational terms, covering its characteristics, its means of acquisition and storage, and media for its processing and transmission.

2. Scope of 'information'

2.1 The term 'information' must be understood in a very broad sense. Information is recognised by its capacity or potential to provide, either directly or indirectly, data or any knowledge, regardless of its physical or intangible character or make-up.

2.2 It further applies to any means of acquiring, transmitting or retaining knowledge or data which may be perceived, acquired, derived or retained by any individual or by the Organisation including by its personnel or equipment in the implementation of the Convention.

2.3 The term 'data' appears in several contexts in the Convention. Generally, 'data' carries the implication of information in a particular structure or format, such as the information embodied in a national declaration. However, in construing the text from the point of view of confidentiality, there is no substantial distinction between 'information' and 'data.' Hence, for the purposes of this policy, the term 'information' will be considered to subsume any references to 'data.' 'Information' or 'data' may include information which is incorrect, false or inaccurate.

2.4 To illustrate the scope of its application, 'information' includes, but is not limited to:

(a) documents with graphic, schematic, numerical, symbolic, pictorial, digital, analogue, photographic or written information;

(b) the products of photography, imagery, inspection, observation, data processing, sampling and analysis;

(c) data stored or displayed on electronic, magnetic or any other physical medium;

(d) information expressed in relative or absolute terms; and

(e) samples and other bodies of chemicals including chemicals carried by earth, dust, filters and sampling, and equipment including sampling, analysis and safety equipment. Samples contain information, and through sample analysis can provide further information.

2.5 Information can be acquired or transmitted through any medium of communications or human sense. Information can be obtained and transmitted due to the mere presence of persons on site or through access granted to them. Thus, equipment, objects, clothes and other personal belongings could become sources of information.

3. Operational definitions of some forms of information

3.1 The following operational definitions, which cover only some forms of information, apply for the purpose of guidelines for handling and protection of information under this Policy. It is to be understood that the following definitions are flexible enough to ensure that handling guidelines can be applied effectively and practically:

(a) **'Document'** could extend to a variety of physical items displaying information or data;

(b) **'Computer material'** includes any computer storage and processing medium. Computer material also covers computing and communications devices, which may be used to record or convey information during an on-site inspection;

(c) **'Audio-visual material'** includes audio and video recordings and digital images; and

(d) **'Sample'** includes a sample's collection medium and any further information acquired or derived from analysis.

3.2 In the application of general operating guidelines to particular items of information falling under these definitions, there may be overlapping reference (for instance, a transparency for overhead projection may be handled as a document or as audio-visual material, and a computer printout may be handled as a document or as computer material).

4. Confidentiality of information under the Convention

4.1 A basic principle on confidentiality, set down in subparagraph 2(c) of the Confidentiality Annex, is that no information obtained by the Organisation in connection with the implementation of the Convention shall be published or otherwise released, except as specifically provided for.

4.2 Specific procedural guidelines in subparagraph 2(a) of the Confidentiality Annex provide that information shall be considered confidential if:

(a) it is so designated by the State Party from which the information was obtained and to which the information refers; or

(b) in the judgement of the Director-General, its unauthorised disclosure could reasonably be expected to cause damage to the State Party to which it refers or to the mechanisms for implementation of the Convention.

4.3 The following factors shall be weighed and carefully balanced by the Director-General or his[*] delegate in determining confidentiality of information:

(a) the potential of its disclosure causing damage to a State Party, any other body of a State Party, including a commercial firm, any national of a State Party, or to the Convention or the Organisation;

(b) the potential of its disclosure offering particular or selective advantage to an individual, a State, or any other body, including a commercial firm;

(c) the basic requirement for effective verification of compliance; and

(d) benefits stemming from the dissemination of general information regarding the implementation of the Convention, in order to promote its acceptance and credibility.

4.4 In determining whether the information it is providing to the Organisation contains confidential information, a State Party could also consider the above factors. The designation of information as confidential shall not undermine the obligation for a State Party to demonstrate compliance with the Convention and shall not be used by a State Party to conceal non-compliance. Furthermore, a State Party cannot prevent the dissemination of information which in accordance with the Convention shall be transmitted in a specified manner to States Parties upon request or routinely.

4.5 Once information has been determined to contain confidential information, it will be necessary to specify the level of sensitivity and scope of access to it. This will be normally done through a system of classification which is set out in Part V of this Policy.

---

[*] Throughout the English version of this Policy, the personal and possessive pronouns ‘he’ and ‘his’ refer without distinction to both the female and the male genders.

5. Relationship of information to the Convention

5.1 The relationship of information to the purposes of the Convention can have implications for how confidentiality measures will apply to that information. Three significant distinctions can be discerned in the implementation of the Convention:

(a) information pertinent to the Organisation to fulfil its responsibilities under the Convention or provided by States Parties to fulfil their obligations under the Convention;

(b) information not related to the aims of the Convention, to which an inspected State Party grants access to demonstrate compliance with the Convention, or which it incidentally discloses in the course of verification activities; and

(c) information, including sensitive information, which is not related to the aims of the Convention, and to which an inspected State Party denies access consistent with its rights and obligations under the Convention.

5.2 Verification procedures and activities need to be guided by these distinctions. However, a judgement as to the relationship of information to the purposes of the Convention could be determined operationally, as the characterisation of information in this way is greatly dependant on individual contexts and circumstances. Obligations to protect confidentiality will be set in relation to information described under each of these distinctions.

PART IV

BASIC RESPONSIBILITIES ON CONFIDENTIALITY

1. Overall responsibilities of the Organisation

The OPCW will receive a great deal of confidential information from States Parties and may be exposed to or acquire more confidential information, often of a more sensitive nature, in the course of verification activities. The OPCW's internal processes will generate further confidential information. This Organisation including its constituent elements therefore must abide by certain obligations to respect confidentiality, in particular:

(a) not to publish or otherwise release information obtained in connection with the implementation of the Convention unless in accordance with the information release procedures as set out in Part VII of this Policy;

(b) to design, plan and carry out verification activities in the least intrusive manner possible, so as avoid disclosure of non-relevant information and to minimise disclosure of confidential information, where this is consistent with effective and timely verification;

(c) to seek and require only the disclosure of information necessary to serve the aims of the Convention, and to specify informational requirements as precisely as possible;

(d) to minimise accessibility of, to protect, and to prevent further dissemination of confidential information not relevant to the Convention which may be incidentally disclosed in the course of verification activities, consistent with effective and timely verification; and

(e) to establish, follow and monitor systematic procedures for limiting the dissemination of and access to information classified as confidential.

2. Responsibilities of the Director-General

2.1 The Director-General is specifically tasked with primary responsibility for the protection of confidential information. The Director-General must establish the regime for handling confidential information within the Secretariat in accordance with the guidelines laid down in the Convention including the Confidentiality Annex and this Policy.

2.2 The Director-General is responsible for supervising adherence to the confidentiality regime within the Secretariat, and must report annually on the implementation of the regime.

2.3 The Director-General has a central role in dealing with breaches and alleged breaches of confidentiality. This includes the establishment of procedures to be followed and

the conduct of investigations in accordance with the Breach Procedures,[3] and the imposition of punitive and disciplinary actions in accordance with the Staff Rules and Regulations. The procedures to be followed should be based on any determinations by the Conference on this subject.

2.4 The Director-General may initiate requests for States Parties to provide "details on the handling of information provided by the Organisation" (CA, (A)4), and consult with States Parties on the form and timing of such requests in accordance with any guidelines set by the Conference. The Director-General could, for instance, request regular reports from all States Parties on their handing of confidential OPCW information.

3. Responsibilities of the Secretariat

3.1 The basic responsibilities of the Secretariat concerning confidentiality derive essentially from the responsibilities of the Organisation and of the Director-General. However, in the practical implementation of the Convention, the definition, conduct and monitoring of the responsibilities of Secretariat staff to safeguard confidentiality are of crucial importance. Particular obligations apply to staff of the Secretariat through their involvement in verification activities and their consequent access to confidential information, both civil and military, which will include information disclosed by a State Party pursuant to its obligations under the Convention, as well as confidential information not relevant to the aims of the Convention in the event that such information is disclosed.

3.2 In addition to the broader obligations already outlined, the Secretariat has the following specific responsibilities:

(a) through the appropriate organisational unit, to evaluate all information it obtains to determine whether confidential information is included;

(b) to establish within a formal position description a specification of the scope of access to confidential information needed for each staff position;

(c) to undertake secrecy agreements with each staff member and to undertake secrecy agreements with authorised bodies outside the Organisation, as necessary;

(d) to maintain a continuing programme of training and awareness for all staff on confidentiality issues, and to monitor each employee's record on protecting confidential information as an explicit element of performance evaluation;

(e) to advise a State Party of a proposed clearance of an employee for access to confidential information that refers to activities on the territory or in any other place under the jurisdiction and control of that State Party, not less than thirty days before access is granted; and

---

[3] Set out in Part IX below.

(f) to handle and store confidential information in a form that precludes direct identification with the facility it refers to, as far as this can be done consistent with effective verification.

3.3 The responsibilities of individual staff members are further defined by a secrecy agreement which must be executed by each employee.

4. Responsibilities of the inspection team

4.1 Particular responsibilities of members of an inspection team stem from the following:

(a) inspectors on site may have access to confidential information;

(b) the inspection team must negotiate with the inspected State Party on certain matters related to confidentiality that require agreement;[4] and

(c) the inspection team is guided by its mandate, draws up an inspection plan, and must decide on specific measures to be employed during the inspection.

4.2 Inspection teams shall therefore:

(a) conduct inspections in the least intrusive manner possible consistent with the effective and timely accomplishment of their mission;

(b) plan the inspection and take into consideration proposals which may be made by the State Party receiving an inspection, at whatever stage of the inspection, to ensure that sensitive equipment or information, not related to chemical weapons, is protected;

(c) fully respect the procedures designed to protect sensitive installations and to prevent the unauthorised disclosure of confidential information;

(d) request only the information and data which are necessary to fulfil the inspection mandate;

(e) prepare an inspection report which only contains facts relevant to compliance with the Convention;

(f) protect and prevent further dissemination of confidential information not relevant to the Convention to which inspection teams have access in the course of on-site inspections; and

(g) respect an inspected State Party's denial of access to sensitive information consistent with the State Party's rights and obligations.

---

[4] For instance in accordance with paragraph 46 of Part X of the Verification Annex and with paragraph 14 of the Confidentiality Annex.

5. Responsibilities of the States Parties

5.1 States Parties must treat information received from the Organisation in accordance with its level of sensitivity as expressed in its classification category. The way this obligation is carried out will naturally differ between States Parties, but as a rule this information should be given at least the same level of protection as that afforded to information with comparable national classification or comparable confidentiality under national legal systems. States Parties shall establish or adapt suitable means of handling and protection of OPCW confidential information in a manner consistent with the principles set out in Part VI of this Policy.

5.2 Each State Party must provide on request details on the handling of information provided to it by the Organisation. This procedure is aimed at promoting general reassurance among States Parties that confidentiality is effectively safeguarded. The responses of States Parties to such requests should at least confirm that standards for handling information are in accordance with paragraph 5.1 above.

5.3 In safeguarding confidentiality of information, States Parties must adhere to the essential obligation to demonstrate compliance with the Convention in accordance with its verification provisions.

5.4 Each State Party must cooperate with and support, to the extent possible, the Director-General in investigating breaches or alleged breaches of confidentiality, and in taking appropriate action in accordance with the elaborated breach procedures should an investigation determine that a breach has occurred. This obligation may include provision of details on the handling of information provided to the State Party by the Organisation and, if necessary, the State Party's participation as one of the disputing parties before the "Commission for the settlement of disputes related to confidentiality" in the event of the breach going before that body.

5.5 The rights and responsibilities of inspected States Parties referred to throughout this policy shall apply, *mutatis mutandis*, to any States Parties which are involved in any other operational deployments including, but not limited to, contingency operations, fact-finding missions and clarification activities.

6. Responsibility of observers

6.1 When, in the course of a challenge inspection, the inspected State Party agrees to grant access to an observer in accordance with paragraph 55 of Part X of the Verification Annex, the observer may have access to some confidential information and will accordingly incur particular responsibilities in relation to its handling and protection. Thus the handling and protection of confidential information by the observer must be fully consistent with all relevant provisions of the Convention, including the Confidentiality Annex, and with this Policy, particularly the detailed handling provisions of Part VI of this Policy. As Article IX, subparagraph 12(a) of the Convention indicates that the observer is a "representative" of the requesting State Party, such information is also subject to the provisions of Article VII, paragraph 6, in respect of both the requesting State Party and the observer as its representative in particular, and hence shall be treated as confidential and afforded special handling.

6.2 Hence the requesting State Party shall be fully responsible for and shall take all necessary measures to ensure that the observer complies with and is individually bound by all relevant provisions of this Policy, as well as to ensure that effective legal remedies and penalties are available in the event of the observer breaching confidentiality, comparable to the measures taken in the event of an official of that State Party breaching confidentiality. Once any confidential information is disclosed to or acquired by the observer, in addition to and without diminishing the observer's own individual responsibility, the requesting State Party also becomes responsible for the handling and protection of that information in accordance with the Convention and with this Policy. For his part, the observer is to adhere to and be bound by all provisions of this Policy relating to the protection of confidential information, and shall not take any unauthorised action in this regard.

PART V

OPCW CLASSIFICATION SYSTEM FOR CONFIDENTIAL INFORMATION

1. Categories of confidential information

1.1 All information acquired or produced by the Organisation and its constituent elements which is determined to be confidential must be given a classification, based on established categories which correspond to the level of sensitivity of confidential information. In its application, the classification system will not impair the requirement for effective verification of compliance with the Convention, and it should be capable of providing, as necessary, for the release of general information, in adequately desensitised form, regarding the implementation of the Convention, in order to promote its acceptance and credibility.

1.2 The essential factors to be considered in determining the level of sensitivity of an item of information are as follows:

(a) the degree of potential damage which its disclosure could cause to a State Party, any other body of a State Party, including a commercial firm, or to any national of a State Party, or to the Convention or the Organisation; and

(b) the degree of potential particular or selective advantage its disclosure could offer to an individual, a State, or any other body, including a commercial firm.

These factors correspond to the factors used in determining the confidentiality of information.

1.3 Based on these guiding factors, and the specific classification criteria set out below, confidential information shall be classified according to the following categories, in increasing order of sensitivity:

(a) **OPCW RESTRICTED**

(b) **OPCW PROTECTED**

(c) **OPCW HIGHLY PROTECTED**

The prefix **'OPCW'** in the names of these categories is used purely to facilitate handling of classified material, in clearly identifying classifications as being those applied by the Organisation and in avoiding any conflict or misunderstanding with distinct national classification systems. The use of this prefix does not imply any particular scope of dissemination.

1.4 There is a distinction between a classification category (which is based on the sensitivity of information) and the scope of dissemination of information (which is based, for instance, on the subject matter, the need-to-know principle, and the particular purpose for which the information is to be used). Level of classification will not prevent the dissemination of information as specifically required by the Convention, including under subparagraph 2(b) of the Confidentiality Annex.

1.5 Information not falling into any of the above-mentioned categories shall be considered not classified and may be marked appropriately. Information which is not classified will be subject to appropriate protection from release by the Organisation and by States Parties, unless specifically cleared for release in accordance with the separately defined release procedures.

1.6 The level of protection afforded to confidential information shall be linked to the level of sensitivity as indicated by its classification category. Each State Party and the Organisation shall protect OPCW classified information originating both from within the Organisation and from States Parties in accordance with its level of sensitivity as expressed by its classification category.

2. Classification category: OPCW RESTRICTED

2.1 CRITERION: This category comprises information of which the unauthorised disclosure would be prejudicial to the effectiveness or credibility of the Convention, or prejudicial to the interests of a State Party or of a commercial or governmental body or of a national of a State Party.

2.2 EXAMPLES: Unless specified otherwise, due to the greater or lesser sensitivity of the data in question, the following forms of information, inter alia, might be classified **OPCW RESTRICTED** when they are acquired or generated by any means by the Organisation:

(a) the initial and annual reports and declarations provided by States Parties under Articles III, IV, V and VI and in accordance with the Verification Annex, where these documents are considered by originating States Parties as being of this level of sensitivity;

(b) general reports on the results and effectiveness of verification activities; and

(c) information to be supplied to all States Parties in accordance with other provisions of the Convention.

2.3 Other information to be classified and handled as **OPCW RESTRICTED** may include: routine confidential correspondence between States Parties and the Secretariat, and internal working documents of the Organisation which are not of particular sensitivity. This may also include information relating to the internal processes and decision-making of the Secretariat, and other managerial or administrative information, where open disclosure of the information might hamper the Organisation’s effectiveness in implementing the Convention.

2.4 DISSEMINATION: **OPCW RESTRICTED** information that must be routinely provided to States Parties in accordance with subparagraph 2(b) of the Confidentiality Annex shall be disseminated accordingly.

3. Classification category OPCW PROTECTED

3.1 CRITERION: This category comprises information of which the unauthorised disclosure may cause substantial damage to the effectiveness or credibility of the Convention, or to the interests of a State Party or of a commercial or governmental body or of a national of a State Party.

3.2 EXAMPLES: Unless specified otherwise in accordance with greater or lesser sensitivity, the following forms of information, inter alia, might be classified as **OPCW PROTECTED** when they are acquired or generated by any means by the Organisation:

(a) the initial and annual reports and declarations provided by States Parties under Articles III, IV, V and VI and in accordance with the Verification Annex, where these documents are considered by the originating States Parties as being of this level of sensitivity;

(b) unpublished technological information about production processes and facilities, and technical information about industrial products;

(c) less sensitive or more general information related to commercial transactions and the cost factors of industrial processes and production;

(d) detailed initial reporting on an inspection, including information on anomalies or incidents at facilities, and inspection reports;

(e) data and information regarding inspection planning of the Secretariat, the inspection goals for a specific facility and travel arrangements;

(f) facility agreements and any attachments thereto; and

(g) information regarding the validation and evaluation of information contained in declarations, facility agreements and inspection reports.

Where such information is not considered relevant to verification of compliance, it will normally be treated initially as **OPCW HIGHLY PROTECTED**, even before any formal classification is determined, as specified in paragraph 4.4 of this Part.

3.3 DISSEMINATION: **OPCW PROTECTED** information that must be routinely provided to States Parties in accordance with subparagraph 2(b) of the Confidentiality Annex shall be disseminated accordingly.

4. Classification category OPCW HIGHLY PROTECTED

4.1 CRITERION: This category comprises sensitive confidential information of which the unauthorised disclosure would cause serious damage to the effectiveness or credibility of the Convention, or its aims and purpose, or cause serious damage from the point of view of national security or commercial secrecy to the interests of a State Party or of a commercial or governmental body or national of a State Party.

4.2 Unless specified otherwise in accordance with lesser sensitivity, the following forms of information, inter alia, might be classified as **OPCW HIGHLY PROTECTED** when they are acquired or generated by any means by the Organisation:

(a) the initial and annual reports and declarations provided by States Parties under Articles III, IV, V and VI and in accordance with the Verification Annex, where these documents are considered by originating States Parties as being of this level of sensitivity;

(b) samples taken from inspected sites and returned samples from designated laboratories, and results from analysis of samples;

(c) especially sensitive confidential information especially provided by a State Party; and

(d) confidential information for which access is normally only required, or voluntarily or incidentally provided, during the actual conduct of an on-site inspection, such as:

(i) process flow diagrams;

(ii) photographs, plans and diagrams of the site;

(iii) specific data related to technological processes and their parameters;

(iv) analytical data of samples taken on site and analysed on site;

(v) commercially sensitive market information, such as a detailed list of customers, and individual quantities sold to them; and

(vi) other detailed, highly specific technical, commercial or national security information.

Where such information is not considered relevant to the verification of compliance, it will normally be treated initially as **OPCW HIGHLY PROTECTED**, even before any formal classification is determined, as specified in paragraph 4.4 below.

4.3 In most inspection scenarios, the highly sensitive information specified in subparagraph 4.2(d) above, that may or may not have a national confidential classification, may be kept at the inspected facility and shall only be made available for on-site use during the inspection. When such information is not taken off site and access to it is limited, there will accordingly be no application of the OPCW classification process within the Secretariat. Even so, during inspection activities the inspection team will give this information at least the level of protection afforded to information as **OPCW HIGHLY PROTECTED**. The classification category of such information should be specified to the extent possible in facility agreements.

4.4 Sensitive information not related to the verification of compliance which is incidentally revealed or collected by any member of an inspection team shall not be

recorded in any form, and shall not be further disseminated. When access is afforded to such sensitive information during inspection activities, any member of the inspection team must give it at least the level of protection afforded to information classified as **OPCW HIGHLY PROTECTED**, until or unless the inspected State Party specifies particular handling or level of sensitivity. In such a case the inspected State Party may designate (as provided in paragraph 5.5 of this Part) an initial classification of such information during the inspection process or in a facility agreement. In the event that such sensitive information is taken to the Secretariat inadvertently or by agreement with the inspected State Party, it shall be classified as **OPCW HIGHLY PROTECTED**, and protected accordingly, unless the inspected State Party specifies otherwise.

4.5 DISSEMINATION: **OPCW HIGHLY PROTECTED** information that must be routinely provided to States Parties in accordance with subparagraph 2(b) of the Confidentiality Annex shall be disseminated accordingly.

5. Classification authority

5.1 For information which has been determined to be confidential and which is transmitted to or generated by the Secretariat, it is mandatory for a classification regime to be applied in accordance with the above categories and guidelines under the direct authority of the Director-General. This regime includes an internal procedure for maintaining consistency of classification for documents generated within the Secretariat, and for consulting on and, if necessary, authorising such classification.

5.2 The classification of such information is to be established by the following authorities:

(a) in the case of confidential information provided by a State Party, that State Party has the authority to designate its classification category;

(i) if a State Party provides information which appears to be confidential without indicating a level of classification, the Director-General or his delegate will be responsible for applying a provisional classification category and treat the information accordingly. He will have the responsibility for consulting promptly with the originating State Party in order to confirm, amend or remove this provisional classification; and

(b) in the case of confidential information generated by the Secretariat, the originator of the information shall be responsible for assigning a provisional classification. The Director-General or his delegate has the authority and responsibility to apply a definitive classification to the information.

5.3 Any document being generated within the Organisation which contains confidential information should provisionally be classified by its originator. In establishing a classification category for a new document that is being generated within the Organisation, due regard should be paid by the originator to the level of sensitivity already established for documents and/or information held by the Organisation and which is pertinent to this new document.

5.4 States Parties, in designating a classification category for confidential information, should take into account its level of sensitivity and the corresponding criteria established for each category described in paragraphs 2.1, 3.1, and 4.1 above. The illustrative indications, set out above, of the forms of information which may be classified under each category do not prejudice the primary authority of a State Party to establish the classification of confidential information it provides.

Classification authority in the course of inspections or other operational deployments

5.5 During the course of an inspection or other operational deployments, or in the formulation of a facility agreement, any State Party which is providing confidential information may designate an initial classification for confidential information, taking into account the level of sensitivity and the corresponding classification criteria. This initial classification will have immediate effect during the conduct of an inspection or other operational deployment and in the transmission of confidential information to the Secretariat at the headquarters on completion of the inspection or other operational deployment. In cases when a State Party discloses to any member of the relevant team sensitive confidential information without establishing a formal classification for it, or when such information is revealed to any member of the relevant team, this member will bear the responsibility of treating this information as **OPCW HIGHLY PROTECTED**, unless the State Party specifies otherwise.

6. Duration of classification

6.1 As a rule, the classification determined for a particular item of information will continue to apply until it is specifically altered or removed in accordance with the guidelines established for reclassification and declassification. When providing confidential information, a State Party may indicate the duration of classification that is to apply to the information. If no indication is given, the duration will be assumed to be unlimited.

6.2 To maintain viable and effective protection of confidential information, to enhance effective verification of compliance and understanding of the whole verification system, and to reduce the archival holdings of formerly sensitive material, States Parties, the Director-General and other originators of such documents within the Organisation may need, inter alia, to keep under review the designation of confidentiality, and the continuing application of classification categories, with a view to either declassification, reduction of classification, or release.

6.3 Classification of information and its duration may be reviewed in particular in the context of a programme for the disposal of records of the Organisation. In carrying out such a programme, the Director-General may from time to time seek the written consent of the originating States Parties in the declassification of records in accordance with agreed procedures. For confidential information generated by the Secretariat, the Director-General shall from time to time review the assigned classifications for holdings of confidential information. If the information refers to any State Party, that State Party will need to provide its written consent before the termination of the duration of the classification. In this respect, an internal review procedure will be established.

7. Change of classification category

Reclassification of confidential information

7.1 The authority to change the classification of an item of confidential information will be the same as that specified in subparagraphs 5.2(a) and 5.2(b**)** of this Part for determination of the original classification of that information. In particular, an item of information supplied by a State Party shall not be reclassified without the written consent of that State Party. This rule will also apply to such items of information contained in documents which had originated within the Organisation.

7.2 States Parties which have originated or received an item of OPCW classified information, and senior Secretariat staff (Branch Heads and above) making use of an item of such information, may request a change in the classification category for that item. Such a request should be based on a clear operational need, and should be acted upon in accordance with the following provisions.

7.3 When the State Party which originated an item of OPCW classified information requests a change of classification, that request will be carried out. Before confirming the change, the Director-General may consult with that State Party on the consequences of the proposed change.

7.4 When there is a request, in accordance with paragraph 07.2 above, for a change in the classification category of confidential information which was generated by the Secretariat, the Director-General or his delegate shall, in making a determination, abide by the criteria established for the application of classification categories with reference to the stated operational need.

7.5 Reclassification of Secretariat-generated information may be required when the information is amended, supplemented or revised so as to create a substantial difference in sensitivity. For instance, a draft report on compliance may have greater sensitivity than the final version, or sensitive material may be omitted in a revised version of an inspection report intended for wider distribution. The principles set out above will be applied in undertaking reclassification, unless the Convention specifies otherwise.

Declassification of confidential information

7.6 The provisions specified above for reclassification of confidential information shall also apply to its declassification. In particular, an item of information supplied by a State Party shall not be declassified without the written consent of that State Party. The following guidelines shall additionally be followed in deciding on the declassification of confidential information:

(a) if declassification is proposed for confidential information originating in the Secretariat and referring to a State Party in a way that influenced its original classification, the Director-General shall obtain the express written consent of the State Party for the declassification; and

(b) for confidential information generated by the Secretariat, the Director-General (or his delegate) shall consider at least the same aspects that he took into account when he designated the information as confidential.

7.7 The declassification of confidential information does not imply that it is, ipso facto, available for public release. Release beyond the Organisation of any information, including formerly confidential information which has been declassified, will require a separate process of consultation and approval in accordance with Part VII of this Policy. This will also apply to information provided to States Parties by the Organisation under an OPCW classification.

PART VI

GENERAL PRINCIPLES FOR HANDLING AND PROTECTION OF CONFIDENTIAL INFORMATION

1. Introduction

1.1 This Part sets out the principles governing the Organisation's provision of access to and regular dissemination of information determined to be confidential, and governing the associated procedures for handling and protection of confidential information. This covers the transmission of confidential information within the Organisation (including its constituent elements), and the transmission of confidential information to authorised representatives of States Parties. Guidelines for public or other release of information beyond the Organisation and States Parties are set out in Part VII.

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, the Manual of Confidentiality Procedure (MCP) and the OPCW Technical Secretariat Information Security Policy. 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.

1.3 The Confidentiality Annex (CA) sets out the two principles governing access to and the dissemination of confidential information within the Organisation:

(a) access to confidential information shall be regulated in accordance with its classification; and

(b) the dissemination of confidential information within the Organisation shall be strictly on a need-to-know basis (CA, subparagraph 2(h)).

1.4 It follows from these fundamental principles firstly that the level of sensitivity of confidential information will govern the procedures by which it is made available to its recipients and the means employed to protect it; and secondly that the authorised recipients of confidential information will be determined in accordance with their demonstrated need, related to the purposes of the Convention. An important consideration in managing the dissemination of confidential information is the scope of access afforded to States Parties: in this context, a primary and unconditional need to know is established by the requirement for data to be provided to all States Parties for them to be assured of continued compliance with the Convention by other States Parties (CA, subparagraph 2(b)). Access to the relevant confidential information

defined by this provision must therefore be provided to serve the vital aim of due transparency and enhanced mutual confidence between States Parties.

1.5 The actual scope of access associated with a certain item of confidential information shall be specifically determined, rather than implicitly assumed, and specific practical steps shall be undertaken in order to protect it against illegitimate or unauthorised access. The rigour of the determination of scope of authorised access and the required level and intensity of protection against unauthorised access shall be regulated in accordance with the classification of that confidential information. However, level of classification does not in itself determine the scope of access to classified information, but simply the manner in which it is to be handled and protected against unauthorised disclosure.

2. Access, dissemination and protection

2.1 The scope of access to confidential information is the full set of possible recipients authorised to acquire or retain that information; dissemination is the process of actively passing that information to its authorised recipients. Accordingly, the notion of 'access' to information entails permitting an individual to acquire or retain that information. Dissemination of confidential information is made possible by the application of protection measures applied in accordance with the level of sensitivity of information, so that it is disseminated to the extent required for the implementation of the Convention without unnecessary or unauthorised disclosure. Accordingly, dissemination of confidential information to all authorised recipients within the Organisation must take place, irrespective of level of classification, with the appropriate protection measures being taken. In this connection, it is notable that States Parties have an obligation under Article VII, paragraph 6, to apply special handling to confidential information received in accordance with the Convention.

2.2 Detailed protection procedures and measures are therefore to be elaborated to permit access to confidential information by an individual Secretariat staff member or by a State Party in accordance with a functional need to know or a specific provision of the Convention, while impeding all other access with a rigour and level of effort linked to the sensitivity of the information as established by its classification. The provision of confidential information to the Conference and to the Executive Council shall be based on the general principles for the dissemination of confidential information.

3. Need-to-know principle

3.1 The need-to-know principle is the governing principle for determination of the scope of access and the recipients of dissemination of information. There is no absolute right within the Organisation to receive confidential information: no individual staff member of the Secretariat and no member of any organ of the Organisation is entitled by virtue of status or level alone to have access to any items of OPCW confidential information.

3.2 Access to confidential information shall normally be granted both on a case-by-case basis and in accordance with the determination of the functional need to know. There is, however, an unconditional requirement for access to certain information by States Parties in accordance with subparagraph 2(b) of the Confidentiality Annex, and this

and related provisions should be viewed as establishing an unquestionable need to know for each State Party, so as to be ensured of the continued compliance of other States Parties with the Convention.

3.3 Within the Secretariat, the specific function or tasks defined for a staff member shall, within practical bounds, be the principal determinant of that individual's need to know and of the consequent scope of authorised access to confidential information.

3.4 The Director-General has the primary responsibility for ensuring the protection of confidential information (CA, paragraph 2). Hence, subject to the provisions of the Convention, the Director-General shall be the final arbiter in the determination of the need to know in relation to any particular items of confidential information.

4. Administration of dissemination and handling procedures

4.1 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 the Head of the OCS. Ultimate responsibility for confidentiality remains with the Director General.

4.2 Once the scope of authorised access to confidential information has been determined on the basis of the need-to-know principle, access shall be granted by means of detailed handling procedures established for the Organisation, to ensure that the manner of access and the level of protection provided are linked to the classification which applies. Each access by a staff member of the Secretariat to a physical medium holding confidential information shall be controlled on a need-to-know basis and shall be recorded, and this record shall be retained. In the event that such access is through an electronic data system, a log-on and log-out procedure shall be established and followed by authorised staff members to ensure that no individual can gain access in the name of another staff member. The OCS will supervise the routine operation of these handling procedures.

5. Determination of scope of access and dissemination of confidential information to States Parties

5.1 There are various circumstances when the Secretariat will need to determine authorised scope of access and consequently to disseminate confidential information to States Parties. In all cases, the governing principle is that established in subparagraph 2(b) of the Confidentiality Annex, and procedures shall be established to ensure that the requirements of this provision are met. Hence, data required by States Parties to be assured of the continued compliance with this Convention by other States Parties shall be routinely provided to them. In particular, information management and clearance procedures shall be followed to ensure that the information which must be provided to all States Parties, in accordance with subparagraph 2(b) of the Confidentiality Annex, is duly provided without further need for consultation and approval within the Secretariat.

5.2 In the case of the provision of certain confidential information to a State Party for a particular purpose, when it is not the application of a specific requirement under the

Convention for dissemination, but is related to a more specific need to know (such as in the course of clarifications under Article IX, paragraphs 3 - 7, or in the settlement of disputes under Article XIV), the general rule is that the Director-General or a single senior official to whom this authority is specifically delegated under the primary responsibility of the Director-General shall be consulted and shall give specific clearance for the proposed access, after confirming the need to know, with the agreement of any State Party to which the information refers and/or which has provided the information. The Director-General shall at all times be kept informed of any exercise of such authority.

5.3 The method of provision of confidential information to a State Party by the Organisation shall be based on the need for continuity of protection, at a level linked to the sensitivity of the information. The receiving State Party is obliged in turn to afford such confidential information the special handling appropriate to its level of sensitivity, and shall provide, upon request, details on the handling of information provided to it by the Organisation.

6. Granting of access to other authorised recipients associated with the Organisation

6.1 It may be necessary to disseminate OPCW confidential information to certain authorised entities or individuals that are outside the Secretariat but are integral to the Organisation's implementation of particular functions specified in the Convention. The Director-General shall establish a stringent regime to govern such access and, in accordance with the Confidentiality Annex, paragraph 2, will retain primary responsibility for any access approved under this regime. Any such proposed access must be specifically authorised by the Director-General or the single senior official specifically delegated this authority under the regime and under the direct responsibility of the Director-General, and then only after a functional need to know has been clearly established for the proposed recipient. The Director-General shall at all times be kept informed of any exercise of such authority.

(a) The Secretariat shall notify a State Party of any such access of those authorised entities or individuals to confidential information in relation to the territory of the State Party or any other place under the jurisdiction or control of the State Party. A specific secrecy agreement providing for protection of confidentiality shall be required as a condition for such access, and this agreement shall be binding on each individual it designates as an authorised recipient. An assessment of the level of protection provided to confidential information by the proposed recipient may be undertaken as a preliminary measure.

(b) The above principle applies to the transfer of samples to designated laboratories under the regime established under paragraph 56 of Part II of the Verification Annex. It may also apply, inter alia, to any access to OPCW confidential information required by an authorised expert (such as may be appointed under subparagraph 4(e) of Article IX or paragraph 8 of Part XI of the Verification Annex) in order to discharge an official function.

(c) In case of access to confidential information by authorised entities and individuals outside the Secretariat, such access shall be strictly limited to the minimum necessary for carrying out functions integral to the Convention's implementation.

6.2 Each person who has been granted access to OPCW confidential information in accordance with this provision shall be responsible for ensuring that any individual beyond the Secretariat to whom he subsequently discloses such information has a functional need to know and also has written authorisation from the Director-General or the delegate (as specified in paragraph 6.1 above) granting the necessary access.

7. Determination of scope of access to confidential information within the Secretariat

7.1 Access to OPCW confidential information within the Secretariat shall be granted only to those for whom such access is necessary for the fulfilment of designated professional duties. In determining need to know within the Secretariat, close attention shall be paid to a staff member's formal position description and specified scope of access to confidential information. An explicit reference to a staff member's particular professional functions is required in permitting access to **OPCW PROTECTED** and **OPCW HIGHLY PROTECTED** information. The authorised scope of access to confidential information classified **OPCW HIGHLY PROTECTED** shall be expressed in writing on a case-by-case basis.

7.2 A register shall be kept of those staff members whose professional duties entail regular access to confidential information relating to each State Party. The Secretariat shall inform a State Party of proposals to accord to an individual staff member access to confidential information in relation to the territory of that State Party or any other place under its jurisdiction or control. The State Party concerned shall be informed not less than thirty days before access is confirmed. Any staffing appointments or changes in personnel structure or functions that will lead to access to confidential information relating to States Parties must be advised to the States Parties concerned not less than thirty days in advance.

7.3 Only certain senior executive staff members shall be authorised to grant access to confidential information to other staff members under their supervision. An administrative directive shall be established by the Director-General which determines the respective criteria according to strict need to know. The granting of access is in each case contingent on a determination that the subject matter is of direct relevance to the proposed recipient's specified duties, with such access always subject to review by the Director-General. In cases of uncertainty about the functional or task-specific need-to-know status of a proposed recipient, a senior staff member with a supervisory responsibility over the recipient must be consulted.

8. Principles for handling and dissemination

Dissemination of confidential information

8.1 The dissemination of confidential information needs to be distinguished from the process of release of information by the Organisation. In general terms, the

dissemination of confidential information refers to the authorised disclosure of such information within the Organisation including all its organs and to the governments of States Parties, including governmental organisations and authorised entities or individuals within States Parties concerned with the operation of the Convention, when this disclosure is essential for specific professional tasks or is in accord with the provisions of the Convention for the furnishing of information to States Parties. With regard to the "release" of information by the Organisation,[5] this process, and its precise scope of application, are defined in Part VII of this Policy.

Acquisition, collection and generation of confidential information

8.2 Specific handling and protective procedures shall be applied on a continuous basis from the first acquisition, collection or generation of confidential information by the Organisation, and to all subsequent activities during its dissemination. Information[6] that may be confidential is acquired, collected and generated by the Organisation in several ways:

(a) information is provided to the Organisation by States Parties:

(i) in conformity with their declaration obligations and reporting requirements specified under the Convention;

(ii) in the course of a formal procedure established under the Convention, such as those included in Article IX; and

(iii) in passing on other information pertinent to implementation of the Convention;

(b) other information pertinent to implementation of the Convention in a State Party may be passed to the Secretariat by that State Party;

(c) information may be passed to the Secretariat or any other organ of the Organisation by a representative of a State Party in the course of a formal procedure established under the Convention, such as those included in Article IX;

(d) information is acquired or collected by an inspection team in the course of an on-site inspection; and

(e) information is generated by Secretariat staff members through the synthesis or other processing of other information, for instance in the course of analysing samples or compiling inspection reports. Generated information may draw on or duplicate information initially provided by States Parties, or may only use

---

5 "Release" of information refers to the approved disclosure of information beyond the Organisation itself (including all its constituent elements) and beyond the governments of States Parties (specifically, beyond governmental organisations and authorised entities or individuals within States Parties concerned with the operation of the Convention (paragraph 1.1 of Part VII of this Policy)).

6 As defined in Part III of this Policy.

information from within the Secretariat. The synthesis of information or the conduct of analysis may produce confidential information which is of a higher level of sensitivity than its original sources.

8.3 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 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 of staff authorised by him to do so. The Director-General has authorised the Head of the OCS to do so.

8.4 Information generated within the Secretariat (such as analytical or other reports, policy papers, profiles, letters, memoranda) which contains confidential information shall be initially classified and so labelled by its originator in accordance with its sensitivity, at a level at least as high as the most sensitive classification of the source material from which it was derived or which was used in the synthesis. Where the level of sensitivity has consequently increased above that of the original source material, a higher level of classification shall be applied.

8.5 Information, including that designated as confidential, which is passed to the Organisation by a State Party must be provided by an official representative of that State Party. The Secretariat will establish and follow a registry process to record the receipt and the official source of such material.

8.6 The classification of information provided by a State Party to the Secretariat would in most cases have already been specified by that State Party, in view of its primary authority for classification. In doing so, the State Party should take into account the level of sensitivity and the corresponding criteria established for each classification category in Part V of this Policy. If a State Party provides the Secretariat with information which appears to be confidential, but without indicating a level of sensitivity, a provisional classification category shall be implemented as provided under paragraph 5.2 of Part V of this Policy.

8.7 The overall obligation to protect and appropriately handle information upon first disclosure to the Organisation is especially important when information is collected during the course of on-site inspections, such as the collection of site-specific observations or the taking of samples. Particular principles for the handling and protection of confidential information during inspections are accordingly set out in section 11 of this Part.

9. Handling procedures for the protection of confidential information

General guidelines on handling and protection

9.1 Individuals shall not discuss or disclose confidential matters in any circumstances when they do not have control over the security of the information and its environment. The Director-General shall establish in an administrative directive specific procedures to prevent unauthorised access and disclosure in conversation or through telecommunication media, with the level of physical or other protective measures linked to the level of sensitivity of the information as expressed in its classification. Actual recourse to the approved use of telecommunications for transmission of confidential information shall be limited to cases of clear operational necessity.

9.2 Subject to the obligation to preclude unauthorised access, Secretariat staff members may disclose confidential information to, or discuss it with:

(a) authorised Secretariat staff members with an established need to know;

(b) persons, who are not staff members and to whom access has been granted under the provisions of paragraphs 6.1 and 6.2 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

(c) authorised representatives of a State Party to which the information pertains, which has the clear entitlement to such disclosure as explicitly established by a provision of the Convention, or for which any other authorisation and need to know have been established.

9.3 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:

(a) hard-copy documents, including papers and paper files;

(b) information in electronic or magnetic form;

(c) computer equipment and systems;

(d) audio-visual material; and

(e) samples.

These administrative directives shall aim at establishing practical mechanisms for ensuring that all the principles established in this document are met.

9.4 For confidential information which relates specifically to inspected or declared facilities, a coding system and associated storage shall be applied to preclude direct identification of any facility to which it pertains, to the greatest extent consistent with effective verification.

10. Specific handling procedures for confidential information

Marking of confidential information

10.1 In order to ensure the proper handling of OPCW confidential information, all documents and media for information storage and processing 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. The basis of the markings will be the three classification categories, one of which should be clearly applied to any medium carrying information determined to be confidential:

(a) **OPCW RESTRICTED**

(b) **OPCW PROTECTED**

(c) **OPCW HIGHLY PROTECTED**

10.2 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 (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.

10.3 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 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 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. The determination of the classification to be applied and the authority to classify must be in accordance with the OPCW Classification System. In cases where information appears to be confidential but is initially not clearly marked by the originator, appropriate marking shall be carried out by the unit, with the determination of a provisional classification category if necessary. Any provisional classification so applied should be promptly confirmed, amended or removed following consultations with the originator of the information.

10.4 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 OCS.

10.5 Information generated by inspectors on the basis of information provided by an inspected State Party, such as inspection reports or parts thereof, shall be marked with the classification which accords with the level of sensitivity indicated by the State Party. In cases where the level of sensitivity of such information is unclear, the information shall be treated as **OPCW HIGHLY PROTECTED** until the level of sensitivity has been clarified through consultations with the inspected State Party.

Filing and record-keeping

10.6 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.

10.7 All confidential information should be stored and internally distributed in a manner that records each staff member who has had access to it, and the date and time of access. The Secretariat shall also establish additional record-keeping procedures to ensure the continuous monitoring of **OPCW HIGHLY PROTECTED** information, and to determine who has had or currently has such information in his possession.

Copying of confidential information

10.8 Copying information entails its replication in a way that generates potential or possible additional access to the information. When copying confidential information, the number of copies made should be kept to a minimum and shall be linked to the approved scope of access and consequent dissemination. The staff member responsible for copying the information must ensure that all copies of a copied document clearly have the appropriate markings.

10.9 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 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.

10.10 Information to be provided to States Parties in accordance with subparagraph 2(b) of the Confidentiality Annex, but which is confidential, shall be copied and disseminated

routinely in accordance with the requests of States Parties and in accordance with an administrative directive issued by the Director-General. In the case of **OPCW PROTECTED** and **OPCW HIGHLY PROTECTED** information, a record should be kept of the number of copies taken and the recipient(s) of each of the copies.

Disposal and destruction of confidential information

10.11 An administrative directive issued by the Director-General shall establish handling procedures for the Secretariat to ensure the secure disposal and destruction of material containing confidential information. These procedures shall cover:

(a) technical methods of destruction or disposal for all categories of media;

(b) registration of destroyed or disposed material;

(c) witness procedures during destruction and disposal; and

(d) reporting requirements for highly classified material provided by States Parties.

Transmission of confidential information

10.12 Transmission of confidential information, in hard copy and electronic format, to and from the Secretariat shall occur in conformity with the level of sensitivity of the information and shall be bound by strict procedures set out in an administrative directive issued by the Director-General. These procedures shall include:

(a) guidelines for secure mailing or manual transmission, and the safe-hand carriage, of confidential information; and

(b) procedures for secure transmission by telephone, telefacsimile, email, file transfer and other telecommunications systems or methods.

10.13 These rules must ensure that for each item of confidential information disseminated:

(a) the item is received at its intended destination;

(b) only authorised users have access to any transmitted data; and

(c) the recipient of a message can verify that the sender is an authorised person.

10.14 An administrative directive issued by the Director-General will describe the standards set down for the secure communications system established for the IMS, and this will be applied in the inspection manual.

Safeguarding of confidential information

10.15 Staff members, and other personnel authorised in accordance with paragraphs 6.1 and 6.2 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. This involves at a minimum following all

the procedures and meeting the standards established within the Organisation for handling and protecting confidential information, and ensuring the continuity of protection during dissemination.

10.16 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 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.

Physical protection and storage

10.17 The Director-General shall set out, in an administrative directive, physical security measures for offices, laboratories, information storage and processing areas, computer media and audio-visual material classified as confidential, as well as standards for physical storage facilities within the Secretariat, including locks and security of secure areas, filing cabinets and sealed containers. These measures shall include procedures for restricting access to OPCW buildings and other sites, and for registering the presence of visitors and staff members during and after working hours. The procedures shall include special access arrangements for especially sensitive areas within the OPCW building(s) and other sites, such as storage areas for confidential information, office areas working with the processing and validation of declarations and inspection reports, the operations centre, computer networks storing and processing confidential information and the OPCW Laboratory.

10.18 Confidential information shall be stored securely at the premises of the Organisation. Some data or documents may also be stored with the National Authority of a State Party. Sensitive information, including, inter alia, photographs, plans and other documents required only for the inspection of a specific facility may be kept under lock and key at this facility (CA, subparagraph 2(e)).

10.19 To the extent practicable, storage of OPCW confidential information at the National Authority of a State Party or at an inspected facility should accord with the minimum standards applied by the Secretariat.

Removal of confidential information from OPCW premises

10.20 Handling procedures shall be established in an administrative directive issued by the Director-General to cover the carriage of confidential information and media from the premises of the Organisation, between sites subject to inspection or other operational deployments and the Organisation, and between the Organisation and representatives of States Parties. Any such removal shall occur only for purposes related to the implementation of the Convention, and only to the minimal extent necessary for the performance of authorised professional functions.

Loss of confidential information

10.21 Procedures shall be set out in an administrative directive issued by the Director-General to cover the eventuality of a loss or suspected loss of OPCW confidential information and media, including loss by an inspector, by a staff member of the Secretariat or by a representative of a State Party, as well as loss in transit. Such procedures shall include requirements for reporting, investigations, and consulting with States Parties concerned. As the loss or suspected loss indicates a possible breach of confidentiality, the procedures for dealing with breaches or alleged breaches of confidentiality must be invoked.

Handling procedures for particular information media

10.22 The handling procedures for confidential information set out in paragraphs 10.1 to 10.21 above apply to all confidential information, regardless of the medium on which it is stored; the following additional procedures relate to information carried on particular forms of media.

Audio-visual material

10.23 An administrative directive shall set out procedures for the handling of audio-visual material containing confidential information, specifying levels of protection in accordance with classification categories, and following closely the procedures specified for handling documents containing confidential information.

Confidential information in computers and computer material

10.24 Access to all sites of the OPCW and key components of the classified computer network, such as the servers, mass storage devices and network communications channels, must be controlled. All hardware in the confidential part of the classified computer network, and especially workstations, servers and user terminals shall be protected from theft, criminal damage, unauthorised physical access, tampering attempts, access denial and other malicious actions. In addition, maintenance and repair activities of the classified computer network's 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.

10.25 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:

(a) access control measures against unauthorised users or any unauthorised external access;

(b) separation of the files and data of the various users; and

(c) 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.

10.26 The data, document and information computer security procedures shall provide detailed guidelines for protecting confidentiality while creating, handling, marking, backing up and destroying all forms of computer files, computer documents and other documents relevant for tasks such as system administration and computer and communications security management and operations.

10.27 Computer material (including portable storage media) and confidential information stored in the OPCW's classified computer network must be handled and protected in accordance with handling and storage procedures supported by detailed technical specifications set out in an administrative directive by the Director-General.

Samples from on-site inspections

10.28 Paragraph 55 of Part II of the Verification Annex provides for the transfer of samples taken during inspections off-site for analysis at designated laboratories. The process of sampling is inherently relevant to the verification of compliance with the Convention, but such samples may also incidentally carry and potentially yield other information which is itself not directly relevant to verification. For this reason, the inspection manual shall include procedures for ensuring the protection of the confidentiality of samples transferred for off-site analysis at designated laboratories.

10.29 Development and implementation of the regime established under paragraph 56 of Part II of the Verification Annex for the collection, handling, transport and analysis of samples shall be founded on the requirement for the protection of confidentiality during the transfer to and storage by designated laboratories. This regime shall address the particular concern that further confidential information not related to compliance might be yielded during the process of compliance-related analysis. Further confidentiality concerns shall be addressed by the sample accounting procedures established under paragraph 57 of Part II of the Verification Annex, and associated procedures for informing the State Party that designated laboratories have destroyed samples or have returned them to the Secretariat after the completion of analysis for appropriate final handling. Designated laboratories shall be required to enter specific secrecy agreements confirming obligations established under the regime governing the sampling and analysis process.

11. Handling and protection of confidential information during operational deployments

Inspection procedures

11.1 All references to inspections, inspection teams, inspectors, and inspected States Parties in section 11 of this Part shall be taken to mean, and shall therefore apply, *mutatis mutandis*, to any other operational deployments including, but not limited to, contingency operations, fact-finding missions and clarification activities.

11.2 The Confidentiality Annex and earlier sections of this Policy establish fundamental principles for the handling and protection of confidential information during inspections, both the information acquired or collected during the verification of compliance, and other information not relevant to the aims of the Convention which may be disclosed in the course of inspection activities. The OPCW inspection manual

is to establish detailed procedures founded on these principles, including the necessary procedures for the use, protection and scope of access of data, documents and files during the conduct of inspections, consistent with the requirements of the Confidentiality Annex and the functional requirements for inspectors in the field. These must take into account functional requirements for the protection of data stored in portable devices, and the general procedures established for the carriage and storage of confidential information.

11.3 The key practical elements for the protection of confidential information in the course of inspections are the inspection procedures, the use of equipment, and the process of consultation within the inspection team and with representatives of the inspected State Party. Inspection procedures shall stipulate a clear hierarchical line of communication within the inspection team to allow consultations on issues that arise in relation to confidentiality, and the use to be made of confidential information. In accordance with this structure, there shall be consultations during facility agreement negotiations, pre-inspection briefings, and during the conduct of initial and subsequent inspections, between representatives of the inspected State Party, the inspected facility and the inspection team, to establish clearly the level of access to be granted to each inspection team member and the treatment to be afforded to confidential information disclosed or collected. In the case of a challenge inspection, an observer is obliged to respect fully the confidentiality of any information to which access is provided in accordance with the Convention's challenge inspection provisions, and shall treat such information accordingly.

Evaluation and classification of confidential information

11.4 The classification procedure set out in paragraph 5.5 of Part V of this Policy shall be applied to information collected during the course of inspection. In accordance with this procedure, such information shall be promptly evaluated for confidentiality, and shall thereupon be given an initial classification and due protection in accordance with its sensitivity, with close reference to any facility agreement and in agreement with representatives of the inspected State Party. Where there is no relevant agreement in place prior to the inspection, the inspected State Party should be encouraged by the inspection team to nominate whenever possible the classification category of any confidential information disclosed during the course of inspection. In the event that sensitive confidential information is disclosed or revealed to any member of the inspection team without any indication of its classification category, the classification system requires that it be handled and protected as **OPCW HIGHLY PROTECTED** unless the inspected State Party provides otherwise. In general, where there is doubt or uncertainty, handling and protection afforded to confidential information should be at the most stringent level applicable, and consultations on further disclosure and dissemination even within the inspection team must fully heed the need-to-know principle for determining scope of access. If collected information includes confidential information not relevant to the Convention, it will require particular handling as discussed in the relevant paragraph below.

Protection of non-relevant confidential information

11.5 This Policy sets out clear principles governing the protection of confidential information not relevant to compliance with the Convention, and the particular responsibilities in this regard.[7] Hence verification activities must be designed, planned and carried out so as to avoid unnecessary disclosure of confidential information and so as to seek to prevent disclosure of such information not related to compliance with the Convention in the terms of any inspection mandate, consistent with effective and timely discharge of verification obligations. These principles also require that confidential information not relevant to compliance with the Convention shall not be sought, recorded or retained: in the course of any inspection, it is a basic responsibility of each member of the inspection team, and especially of its leader, to ensure that this does not occur. However, it is recognised that in the course of inspection activities, it might occur that other confidential information which is itself not relevant to the purpose of the inspection is collected or recorded in various forms (as are set out in the definition of "information" in Part III of this Policy),[8] by means of items such as approved inspection equipment, inspectors' clothing, and personal articles. In the event that such information is disclosed in the course of inspection activities, it shall not be further disseminated in any form, even within the inspection team, and shall be returned to the inspected State Party or destroyed under its supervision.

11.6 In the course of inspection activities, the Confidentiality Annex specifies that States Parties "may take such measures as they deem necessary to protect confidentiality, provided that they fulfil their obligations to demonstrate compliance in accordance with the relevant Articles and the Verification Annex".[9] Inspection teams are obliged, among other things, "to take into consideration proposals which may be made by the State Party receiving the inspection, at whatever stage of the inspection, to ensure that sensitive equipment or information, not related to chemical weapons, is protected".[10] "Inspection teams shall strictly abide by the provisions set forth in the relevant Articles and Annexes governing the conduct of inspections. They shall fully respect the procedures designed to protect sensitive installations and to prevent the disclosure of confidential data."[11]

11.7 Subject to a full consultation process with the inspected State Party both during and after an inspection (such as is established for challenge inspections in paragraph 61 of Part X of the Verification Annex), the Organisation is responsible for confirming to the inspected State Party that information gathered in accordance with the provisions of the Convention in the course of inspection activities is relevant to compliance with the Convention in the terms of the inspection mandate. The inspection team must protect any information gathered during the inspection in accordance with the classification level which the inspected State Party prescribes for it. The inspected

---

7 Set out in section 4 of Part IV of this Policy.

8 Set out in section 2 of Part III of this Policy.

9 Confidentiality Annex, paragraph 13.

10 Confidentiality Annex, paragraph 14.

11 Confidentiality Annex, paragraph 15.

State Party may not, within the framework of existing obligations in relation to demonstration of compliance with the Convention, object to inclusion of information in the preliminary inspection findings, if following full consultations the inspection team maintains that it is relevant to compliance with the Convention in the terms of the inspection mandate.

11.8 Any information gathered in the course of inspection but not included in the listed and copied material provided to the inspected State Party is presumed not to be relevant to the inspection mandate, and must be treated as specified in paragraph 11.5 above. The principle is recognised that limitations on access and dissemination, such as those agreed as part of managed access in the case of a challenge inspection, shall be complied with by inspection team members and that no information a State Party views as confidential but of which it has not received a copy will leave the inspection site without its consent. Without prejudice to the obligation for a State Party to demonstrate compliance, procedures to implement the above principles include, inter alia:

(a) additional cleaning of inspection equipment;

(b) changing of clothes before or after a particular inspection activity;

(c) leaving personal articles behind before entrance to a particular area;

(d) the transfer of affected equipment under joint seal to the Secretariat for decontamination under the supervision, if requested, of a representative of the inspected State Party;

(e) the retention on site of detachable parts carrying confidential information unrelated to the Convention; or

(f) after exploring all other possibilities, including the above, the retention of equipment on site.

These procedures shall not be abused and shall be implemented, where relevant, in accordance with a legal framework respecting the immunity established under subparagraph 11(d) of Part II of the Verification Annex.

11.9 None of the procedures followed in accordance with these principles shall impede or delay verification activities conducted under the inspection mandate and in accordance with the provisions of the Convention.

PART VII

PROCEDURES FOR THE RELEASE OF INFORMATION BY THE OPCW

1. General

1.1 This Part of this Policy sets out the principles governing the procedures which the Organisation is to follow concerning the release of any information which it holds in connection with the implementation of the Convention. 'Release' of information by the Organisation refers to the approved disclosure of information beyond the Organisation itself (including all its constituent elements) and beyond the governments of States Parties (specifically, beyond governmental organisations and authorised entities or individuals within States Parties concerned with the operation of the Convention). Accordingly, these principles govern the release of OPCW information to any other international organisation, to the government of a State not party to the Convention, to private or governmental organisations unrelated to the implementation of the Convention, or to any individual who is neither employed or contracted by the Organisation nor authorised by a State Party in relation to implementation of the Convention.

1.2 In the course of the implementation of the Convention, there will be cases in which the Organisation needs to release information in order to comply with its obligations. The release may be fully public, or may be limited in scope according to particular circumstances. The need to release information may arise for both unclassified and classified information. No information obtained or generated by the Organisation in connection with the implementation of the Convention shall be published or otherwise released, except in accordance with the following guidelines.

2. Public release of information

2.1 The Director-General may publicly release information that is not designated as confidential (including formerly confidential information which has been declassified in accordance with paragraphs 7.6 and7.7 of Part V of this Policy) and that falls into one of the following categories:

(a) general information on the course of the implementation of the Convention which does not contain material relating specifically to any State Party. This excludes specific information about inspection activities being conducted in or planned for a State Party. The types of information which may be released publicly under this provision will be set out in a list approved by the Conference; this list could include details of declaration requirements and forms, generic or model documentation, summary information about the overall verification programme, and verification technology and methodology applied in on-site inspections;

(b) factual organisational information about the Organisation, except for information that relates to the security of the Organisation, or to personnel matters and the privacy of staff of the Secretariat; or

(c) information referring to a State Party, which is unclassified and which that State Party has specifically requested or consented to be publicly released.

2.2 The Director-General shall consider and decide upon individual requests for the public release of information, provided that it falls within the terms of the preceding paragraph. Requests going beyond these parameters shall be referred to the Executive Council or the Conference for decision.

2.3 All contacts between Secretariat staff members and the media shall be subject to this Policy, in particular, Part VII of this Policy (including these procedures established for the public release of information) and the OPCW Media and Public Affairs Policy. The Director-General shall issue an administrative directive governing media policy, in accordance with these public release policy guidelines.

3. Limited or non-public release of information

3.1 There may be cases where it is necessary[12] to release information beyond the Organisation in a manner that is short of full public release. This may include release to an international organisation or governmental organisation for official use only, and subject to certain conditions. Such non-public release may apply to confidential information bearing an OPCW classification, or to declassified as well as to unclassified information. Confidential information bearing an OPCW classification shall be released only if the Director-General confirms that adequate protection and control can be maintained in the recipient organisation. The Director-General shall conclude an agreement or agreed arrangements with potential recipient organisations on the handling and protection of classified information.

3.2 Limited or non-public release of information might take place:

(a) when the Executive Council decides to bring an issue or matter directly to the attention of the United Nations General Assembly and the United Nations Security Council in accordance with paragraph 36 of Article VIII;

(b) when the Conference decides to bring an issue to the attention of the United Nations General Assembly and the United Nations Security Council in accordance with paragraph 4 of Article XII; or

(c) when the Conference or the Executive Council decides to request the opinion of the International Court of Justice with the authorisation of the General Assembly of the United Nations in accordance with paragraph 5 of Article XIV.

3.3 The limited or non-public release of information which does not bear an OPCW classification can be authorised by the Director-General provided that the information falls within the categories set out in paragraph 2.1 of this Part. Requests for the release of information not bearing an OPCW classification but going beyond these parameters shall be referred to the Executive Council or the Conference for decision.

---

[12] In accordance with subparagraph 2(c) of the Confidentiality Annex.

3.4 When limited or non-public release is proposed for confidential information, the scope and conditions for such release shall be in strict conformity with the needs of the implementation of the Convention. The need-to-know principle governing dissemination of information must still apply.

3.5 If confidential information refers to a particular State Party, and that State Party expressly requests or consents to its release, then the release may proceed without further consultation. In all other cases, a decision of the Conference or the Executive Council is required for the release of confidential information beyond the Organisation. While a request for a decision on such a release can be put to either organ, such a request will normally be part of a general policy decision by the Conference or Executive Council to refer a related issue to an external body in accordance with the Convention, and so the decision on release would be taken by the same organ considering the general policy question.

3.6 A decision to approve such a release should be based upon:

(a) an explicit determination that the intended recipient has a clear need to know in accordance with the recipient's role in the implementation of the Convention; and

(b) a determination that the intended release conforms with the needs of the Convention.

3.7 When an apparent need arises for release of confidential information, the Director-General shall prepare a draft proposal for release for consultation and review by the parties concerned. The factors for determining confidentiality and the classification of the information are required to be fully addressed in the formulation of the proposed release. When applicable, the information proposed for release shall be processed into less sensitive forms so that disclosure of confidential information not relevant to the purpose of the release is avoided. In this case the processes for declassification or reclassification should be applied. If the confidential information was obtained from or refers to a State Party, the Director-General or a delegate authorised for this function is required to obtain the written consent of that State Party for the proposed release. The withholding of such consent shall not be used to avoid a State Party's obligations under the Convention.

3.8 In preparing a release proposal, the Director-General may propose specific conditions or limitations on the scope to be associated with the release, with the aim of ensuring that the release is focused on its particular purpose connected with the implementation of the Convention. Some of the limitations of scope or conditions that may apply are:

(a) access to the confidential information only on a temporary basis, such as for the duration of a meeting or for the duration of a consultancy;

(b) specification that the information is for official use only;

(c) request for particular handling, such as a request to destroy or return the information after a specified period;

(d) specific controls on some sensitive parts of the confidential information; and

(e) visual display of the confidential information, such as projection during the course of a meeting.

3.9 After consultation with the parties concerned, the proposal for release will then be put to the Executive Council or the Conference for decision.

PART VIII

ADMINISTRATION

1. The Director-General

1.1 The Director-General shall establish and supervise the implementation and auditing of the regime for the protection and handling of confidential information within the Organisation in accordance with the principles set out in the Confidentiality Annex and this Policy. To this end, the Director-General shall issue and supervise the implementation of administrative directives required by this Policy.

1.2 The Director-General shall have the primary responsibility for the enforcement of this regime and will charge appropriate units in the Secretariat with particular tasks for the implementation of the regime in accordance with this Policy. In exceptional cases, the Director-General may delegate specific authority in relation to implementation of the confidentiality regime to a limited number of senior Secretariat staff members, subject to specific limitations set out in this Policy.[13] The Director-General shall also personally supervise the conduct of those units and shall remain personally responsible for actions taken by his delegates in exercising his authority.

2. Administration of the confidentiality regime in the Secretariat

2.1 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 4.3 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.

2.2 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 in any event as soon as possible after the introduction of the structural change in question.

---

[13] Refer in particular to paragraph 5.2 and section 6 of Part VI of this Policy.

PART IX

BREACH PROCEDURES

1. Breach investigation procedures

Investigations into breaches and alleged breaches of confidentiality and violations of confidentiality obligations

1.1 On the basis of the provisions of the Confidentiality Annex (paragraph 19), this Part of the Policy outlines the procedure for investigations by the Director-General in relation to breaches and alleged breaches of confidentiality and violations of related obligations to protect confidential information.

Step 1: Investigation by the Director-General
Step 2: Interim action
Step 3: Report of investigations
Step 4: Action in response to an investigation report
- 4a: Disciplinary sanctions against serving Secretariat staff
- 4b: Sanctions against former Secretariat staff
- 4c: Action taken in relation to waiver of immunity
- 4d: Other legal action within national jurisdiction
- 4e: Action taken when a State Party appears responsible
- 4f: Action to reform or enhance the confidentiality regime

Definitions

1.2 A breach of the obligation to protect confidentiality (‘a breach of confidentiality’) includes any unauthorised disclosure of OPCW information to any individual, or government or private entity, regardless of the intention or the consequences of the disclosure. A breach of confidentiality can also be associated with misuse of information to gain a personal advantage or to benefit or damage the interests of a third party. A violation of obligations concerning the protection of confidential information is deemed to have taken place if there has been non-compliance with the specified procedures for the handling, protection, release and dissemination of confidential information so as to create a clear risk of unauthorised disclosure, with or without such disclosure actually occurring. In practical terms, there is considerable overlap between a breach of confidentiality and a violation of obligations to protect confidential information.

Step 1: Investigation by the Director-General

1.3 As required in the terms of the Confidentiality Annex, the Director-General shall promptly initiate an investigation:

(a) following 'sufficient indication'[14] that there has been a violation of an obligation to protect confidential information on the part of a staff member or contracted personnel of the Secretariat, another authorised individual or entity beyond the Secretariat , or an agent or official of a State Party; or

(b) when a State Party has lodged an allegation concerning a breach of confidentiality.

1.4 In particular, the Director-General shall initiate an investigation if he becomes aware that there is a reasonable possibility, or clear risk, of unauthorised disclosure of confidential information occurring, inter alia, in a manner:

(a) which violates the policy or guidelines of the Organisation established for the handling, protection, release and dissemination of confidential information; or

(b) which could adversely affect the object and purpose of the Convention or the interests of the Organisation, a State Party, or a commercial or governmental body or a national of a State Party, or could offer particular or selective advantage to an individual, a State, or any other body, including a commercial firm.

1.5 The Director-General is obliged to investigate any allegation by a State Party that a breach of confidentiality has occurred. Such an allegation should be made in writing to the Director-General, and should to the extent possible provide supporting information. An allegation should, if possible, state the nature of the information involved, the time and location at which the breach is alleged to have occurred, and the actual or possible future damage believed to affect relevant interests.

1.6 When a decision has been taken by the Director-General to proceed with an investigation, the decision should be made known immediately in writing to any States Parties and any Secretariat staff member or contracted personnel involved in the alleged breach or suspected violation.

1.7 The aim of the investigation is to establish whether there has been a breach of confidentiality or a violation of the handling, protection, dissemination or release procedures for confidential information, and the severity of any breach including the degree and nature of any damage caused. The investigation should also consider ways of enhancing the confidentiality regime so as to prevent any recurrence of a breach or violation of procedures.

---

[14] A sufficient indication that there has been a violation of an obligation to protect confidential information exists when based on facts that can be articulated, there can be a reasonable belief that a violation has occurred.

1.8 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. The investigation should commence with a preliminary review of the circumstances surrounding the allegation or indication of a violation, and a consideration of any evidence or supporting information. The Director-General at this stage may find that a *prima facie* case[15] does not exist; if so, he may, at his discretion, either consult with a State Party that has made an allegation, or he may conclude the investigation and report a finding that no *prima facie* case was established. Following the establishment of a *prima facie* case of a breach affecting the interests of a State Party, the Director-General shall notify the Executive Council that an investigation into a breach is in progress and, with the consent of that State Party, may present specific information about the investigation, if requested.

1.9 The investigation procedure following the establishment of a *prima facie* case may include the following activities:

(a) the collection and examination of evidence within the OPCW or its constituent organs;

(b) the examination of further material supplied by States Parties as evidence;

(c) confidential interviews with staff members of the Secretariat;

(d) consultations with States Parties concerned, including with representatives of industry or private entities concerned nominated by States Parties; and/or

(e) a request for a State Party to provide details on the handling of information provided to it by the Organisation.

1.10 The proceedings of the investigation will remain confidential, and will be subject to the strict application of the need-to-know principle. Particular care should be given to the possible damaging effects of disclosures about such an investigation to Secretariat staff members as well as to the interests of States Parties. The investigation should be conducted on the basis of objectivity and due process, and there should be no use of coercion to elicit information from any individual concerned. Every effort should be made to conclude the investigation and take appropriate action in response to its findings as quickly as is possible and consistent with proper procedure.

1.11 All States Parties concerned and all staff members of the Secretariat involved shall cooperate with and support the investigation to the extent possible. For States Parties, this may entail providing details of internal investigations conducted, furnishing evidence, advising on national judicial proceedings in relation to the same matter, and advising on the degree and nature of damage caused by a breach. Staff members are required to provide any factual information relating to the aims of the investigation and their professional responsibilities.

---

[15] A *prima facie* case exists when an allegation has been made with enough evidence that, if true, it could lead a reasonable decision-maker to conclude that a violation had occurred.

Step 2: Interim action

1.12 If a *prima facie* case is established which apparently implicates a currently serving member of the Secretariat:

(a) procedures will be initiated in accordance with the Staff Regulations and Rules to impose interim restrictive measures for the duration of the investigation, such as withdrawal from certain functions, suspending the payment of any salary, entitlements, benefits and/or emoluments, or denial of access to certain information, or, if the case appears serious, temporary suspension in accordance with the OPCW Staff Regulations and Rules;

(b) the Director-General shall consider and may propose immediate action, if necessary in consultation with the Executive Council, to protect all legitimate interests which could be prejudiced by the breach or alleged breach of confidentiality, including the interests of a State Party or of the Organisation; and

(c) if the investigation is at the request of a State Party, then the Director-General shall inform this State Party of any such interim action taken.

1.13 A staff member suspected of involvement in a breach should be informed by registered letter of the decision to take such interim action, stating the basis of this action and advising of any recourse available.

1.14 If the preliminary stage of the investigation discloses *prima facie* indications that a State Party may have been responsible for a breach, or may have otherwise been involved, the Director-General shall consider and may propose immediate action for decision of the Executive Council, to protect all legitimate interests which could be prejudiced by the breach of confidentiality, including the interests of any other State Party or of the Organisation. The Director-General may request that State Party to provide details on the handling of information provided to it by the Organisation.

1.15 If the preliminary stage of the investigation discloses *prima facie* indications that a natural or legal person in a State Party's jurisdiction may have been responsible for a breach, or may have otherwise been involved, the Director-General may consult with and request support from that State Party, if necessary following Executive Council approval, on possible action to protect all legitimate interests which could be prejudiced by the breach of confidentiality.

1.16 The Director-General is empowered to take the interim actions set forth in this section at any time from the establishment of a *prima facie* case until the conclusion of the investigation.

Step 3: Report of investigations

1.17 The Director-General shall prepare a report of the investigation which will state whether there has been a breach of confidentiality or a violation of the handling, protection, dissemination or release procedures for confidential information. The report will be prepared in two forms, a full form which sets out the facts determined in

detail, and a modified form from which specific confidential material has been removed to ensure that confidential information connected with a breach is not further disclosed beyond its authorised scope of access, and to respect those elements of the privacy of individual staff members not relevant to the case.

1.18 The full report shall be treated as confidential, to be classified and handled according to its sensitivity. It should be made available only to all those who are directly involved in the investigation, including any individual staff members implicated in a breach or alleged breach, and any State Party making an allegation of a breach. In its modified form, the report may be made available to any State Party upon request and it shall be summarised in the annual report of the Director-General to the Conference concerning confidentiality as required under paragraph 3 of the Confidentiality Annex. Where possible, the report should, in both forms, contain concrete proposals for the enhancement of the confidentiality regime. If the Director-General requested the Executive Council to approve interim action in accordance with paragraphs 1.12,1.14, or 1.15 of this Part, then he should report directly to the Executive Council on the implementation of interim action.

1.19 When the report finds that there has been a breach of confidentiality, there should be an account of the degree of severity of the breach, with reference to the following factors:

(a) whether the breach occurred through deliberate or accidental steps, or through negligent omission;

(b) whether the breach involved a violation of obligations under this Policy and associated administrative directives, or of specific agreements such as a staff secrecy agreement or a facility agreement;

(c) the degree of actual or potential damage, if any, to the interests of any party concerned; and

(d) the degree of any private advantage gained through the unauthorised disclosure or consequent misuse of information, in particular promoting self-interest, competitive advantage, the benefit of a third party, or an intention to damage a third party's interest.

1.20 If the State Party requesting an investigation is not satisfied with the report issued by the Director-General following an investigation, and after all reasonable attempts have been made to resolve the issue through consultations, that State Party has the right to request that the Confidentiality Commission be convened to consider the case.

1.21 If the investigation has not been completed within three months of the initial decision to proceed, the Director-General should make an interim progress report to those who receive the final report in its full form, with the exception of the subjects of the investigation themselves. This report should set out the steps taken to that date, and any obstacles or reasons for delay in completing the investigation. If, after consultations, it subsequently appears that these obstacles or delays cannot be expediently overcome, the Director-General may conclude the investigation and in his

report request that the Confidentiality Commission be convened to consider the case in accordance with paragraph 23 of the Confidentiality Annex.

1.22 If, on conclusion of the investigation, it is determined that a breach or violation has not occurred, the Director-General's report should include a statement exonerating the accused Secretariat staff member or State Party.

Step 4: Action in response to an investigation report

1.23 An investigation and report which finds that there has been a breach or violation may lead to four broad categories of possible response:

(a) disciplinary actions internal to the Organisation and covering current staff of the Secretariat, and sanctions covering former staff members;

(b) legal proceedings conducted under the national jurisdiction of a State Party, following the waiver, when relevant, of any immunity from jurisdiction;

(c) reform or enhancement of the OPCW confidentiality regime; and

(d) other action when a State Party appears responsible.

Step 4a: Disciplinary sanctions against serving Secretariat staff

1.24 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.

1.25 The severity of the breach and the degree of individual responsibility should be weighed in determining which measures should apply to a staff member.

1.26 The decision of the Director-General concerning disciplinary action may be subject to review or appeal, in accordance with procedures established under the OPCW Staff Regulations and Rules.

Step 4b: Sanctions against former Secretariat staff

1.27 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 one or more of the following disciplinary measures:

(a) Written censure;

(b) Barring the former staff member from any future employment at the OPCW; and/or

(c) The loss of financial or other entitlements, such as those related to the OPCW Provident Fund.

1.28 The Director-General will not be required to seek the recommendation of the Joint Disciplinary Committee before deciding on the application of any of the foregoing disciplinary measures.

Step 4c: Action taken in relation to waiver of immunity

1.29 Separate from these disciplinary measures, the Director-General may decide to waive immunity from prosecution. This applies both to currently serving Secretariat staff members of the Secretariat, and to former staff members who may retain immunity relating to actions taken during their term of service with the Secretariat. Waiver of immunity is to be considered only in the event of a serious breach, when individual responsibility has been established and damage has been suffered as a result thereof, and should ensue in conjunction with confidential consultations as to the possibilities of relevant national jurisdiction being applied. The individual secrecy agreement signed by the staff member should also be reviewed for its possible use in legal action.

1.30 Any decision to waive immunity may be subject to review or appeal in accordance with the procedures established under the OPCW Staff Regulations and Rules.

1.31 States Parties shall take appropriate legal action, to the extent possible, in making an appropriate response to the waiver of immunity. The action to be taken will be in accordance with section 3 of this Part, including possible legal proceedings that may apply to the present or former staff member whose immunity is waived. If the present or former staff member responsible for a breach is residing or is otherwise within the jurisdiction of a State not Party to the Convention, the Director-General may seek the authority of the Executive Council or the Conference to undertake consultations with the aim of encouraging that State to initiate or facilitate appropriate action to support legal processes resulting from the breach.

Step 4d: Other legal action within national jurisdiction

1.32 If the investigation by the Director-General determines that a natural or legal person (including a commercial entity) under the jurisdiction of a State Party appears to have been responsible for a breach of confidentiality, has derived particular advantage from a breach of confidentiality, or has otherwise been involved in a breach of confidentiality, that State Party may be required to take appropriate legal action in accordance with section 3 of this Part.

1.33 If a legal or natural person found responsible for a breach is residing or is otherwise within the jurisdiction of a State not Party to the Convention, the Director-General may seek the authority of the Executive Council or the Conference to undertake consultations with the aim of encouraging that State to initiate or facilitate appropriate action to support legal processes resulting from the breach.

Step 4e: Action taken when a State Party appears responsible

1.34 If the investigation by the Director-General determines that a State Party, including an official of a State Party, appears to have been responsible for a breach of confidentiality:

(a) that State Party shall assist the Director-General to resolve the matter, to the extent possible, including providing full details of its handling and protection of confidential information supplied by the Organisation;

(b) that State Party shall take appropriate legal action in accordance with section 3 of this Part; and

(c) the Director-General may raise the matter with the Executive Council and request further action in response to the investigation report.

1.35 A State Party's possible responsibility is to be assessed in the light of its obligations under the Convention, particularly paragraph 6 of Article VII and paragraph 4 of the Confidentiality Annex.

1.36 If an investigation finds that a State Party appears responsible for a breach, the Confidentiality Commission may be convened in case of disputes to consider the case in accordance with paragraph 23 of the Confidentiality Annex and the detailed procedures established for the Confidentiality Commission.

1.37 Where the investigation discloses a breach of confidentiality involving the interests and actions of States Parties only, the Director-General shall inform the States Parties concerned of such an outcome.

Step 4f: Action to reform or enhance the confidentiality regime

1.38 The report of the investigation should contain concrete proposals for the reform or enhancement of the protection of confidential information within the Organisation, both specifically to prevent the recurrence of any breach or violation established by the investigation, and on the basis of other observations about the general protection of confidentiality which may emerge from the investigation.

1.39 The Director-General should recommend to the Conference for adoption at its next meeting any proposals for reform or enhancement of this Policy or other basic policy documents that emerge from the investigation.

1.40 If the investigation demonstrates a need for improved handling and protection procedures, or any other alteration of the working procedures of the Secretariat, the Director-General shall issue appropriate administrative directives to implement these changes without delay.

2. Rules Governing the Commission for the Settlement of Disputes Related to Confidentiality ("the Confidentiality Commission")

Rules governing the composition of the Confidentiality Commission

2.1 The Confidentiality Commission as a whole will be made up of persons appointed in a personal capacity from a list of nominees put forward by States Parties to the Convention. Each State Party may nominate one of its citizens who is available and qualified to serve on the Confidentiality Commission. This list of nominees will be submitted to the Conference and 20 persons shall be appointed from it to serve on the Confidentiality Commission for an initial two-year term.

2.2 The 20 appointees are to be determined through a process of consultation with regional groups under the direction of the Chair of the Conference: these consultations shall take into account the principle of rotation and the need for a comprehensive spread of relevant fields of expertise, to result in the designation of four nominees from each of the five regions defined in paragraph 23 of Article VIII of the Convention by the States Parties belonging to the respective regions. Due appointment of these nominees to the Confidentiality Commission shall then be taken by the Conference as a decision on a matter of substance, in accordance with Article VIII, paragraph 18 of the Convention.

2.3 Nominees should be proposed by States Parties on the basis of individual competence, integrity and background in one or more fields relevant to the work of the Confidentiality Commission, such as dispute resolution of various types; the confidentiality and verification provisions of the Convention; the chemical industry; military security; data security; international law; and national legal systems.

2.4 The Confidentiality Commission as a whole shall meet for an inaugural meeting during the course of the first Conference at which it shall, by consensus, elect its Chair from amongst its members to serve for an initial term of one year. Thereafter, the Confidentiality Commission shall hold a regular annual meeting, in conjunction with the regular annual session of the Conference, during which the Confidentiality Commission will elect its Chair ('the Chair') for the coming year in accordance with the operating procedures approved by the Conference.

Disputes the Confidentiality Commission may deal with

2.5 The Confidentiality Commission may be called upon to deal with disputes in the following circumstances:

(a) when invoked to consider disputes arising from a breach or breaches of confidentiality involving both a State Party and the Organisation;

(b) when, in accordance with Article XIV, paragraph 4, of the Convention, the Conference of the States Parties entrusts it with a dispute relating to confidentiality other than a dispute such as those identified in subparagraph 2.5(a) above; or

(c) when chosen by two States Parties in dispute over a matter of confidentiality as a means of resolving their dispute pursuant to Article XIV, paragraph 2 of the Convention.

Rules governing the operating procedures of the Confidentiality Commission

2.6 These rules were approved by the Third Session of the Conference and govern the detailed operating procedures for the Confidentiality Commission.

Commencement of the dispute resolution process

2.7 In the event of the Confidentiality Commission being called upon to deal with a dispute in the circumstances set out in paragraph 2.5 above, the matter will immediately be forwarded to the Chair, who shall in turn immediately inform all members of the Confidentiality Commission about the case. The Chair shall then consult with all members of the Confidentiality Commission on the timing and process for resolving the dispute, including convening meetings as necessary, in accordance with procedural guidelines in the operating procedures which take into account such factors as indications of gravity or urgency on the part of a disputing party, the complexity of substantive issues involved, the scale of alleged loss or damage, and the need for minimising the scope of further access to confidential information. At the conclusion of these preliminary steps, the Chair shall obtain the agreement of the Confidentiality Commission on a proposed timetable and a process for resolution for the dispute.

Seeking a mutually agreeable resolution

2.8 The Confidentiality Commission shall initially aim at clarifying the basis of the dispute and at resolving the dispute in a manner that is acceptable to the disputing parties and that is consistent with the rights and obligations of States Parties and the Organisation under the Convention. In making every effort to encourage disputing parties towards a mutually satisfactory outcome, the Confidentiality Commission should adopt a means of dispute resolution appropriate to the case, which takes account of any common preference of the disputing parties: for instance, the initial means adopted would preferably comprise a mediation process practically geared to reaching an agreed settlement through negotiation.

2.9 To this end, the Confidentiality Commission may form an advisory committee to undertake informal mediation consultations; normally this advisory committee should be composed of five Confidentiality Commission members, one from each region, unless the disputing parties agree to request a similar, modified structure which they believe would serve better to reach a mediated resolution. Any such committee must report to the Confidentiality Commission on the progress and result of any consultations, and any possible mediated resolution derived from this process must be put to the Confidentiality Commission to be certified.

2.10 If, by any appropriate means, the Confidentiality Commission reaches a mediated resolution of the dispute acceptable to the disputing parties, this outcome shall be certified by the Confidentiality Commission and a factual statement on the outcome shall be provided to the disputing parties for their agreement to be recorded.

Absence of mutually acceptable resolution

2.11 If no such outcome can be reached, the Confidentiality Commission shall prepare a report outlining the basic facts of the dispute, commenting objectively upon the dispute and recommending further action that might be taken to resolve it, by the disputing parties themselves, by the Confidentiality Commission, by the Conference, or by another organ of the Organisation, in accordance with a specific mandate from the Conference. This report shall be passed by the Confidentiality Commission to the disputing parties. The report and recommendations of the Confidentiality Commission shall not be binding on the disputing parties, but may provide a basis or rationale for further action on the part of the disputing parties or competent organs of the Organisation: in particular, the Confidentiality Commission may refer the matter to the Conference, or to another organ of the Organisation in accordance with a specific mandate from the Conference and if the disputing parties concur that this is necessary due to the urgency of the case.

2.12 If two disputing States Parties agree as a condition of referring a dispute to the Confidentiality Commission, the Confidentiality Commission may, with the explicit consent of the disputing parties, decide on an arbitrated resolution to the dispute which is binding on the disputing parties.

2.13 In preparing its reports and recommendations, the Confidentiality Commission shall take into account the need-to-know principle governing access to confidential information and the specific procedures adopted by the Confidentiality Commission to ensure that confidentiality remains protected in the exercise of its functions. Confidentiality Commission members shall themselves be bound by all obligations under the Convention and this Policy in relation to handling and protection of confidential information.

Reporting to the Conference

2.14 The Confidentiality Commission shall remain responsible to the Conference, and shall report on its activities in the preceding year at every regular session of the Conference. This report shall include the number of mediated and arbitrated resolutions reached, the categories of disputes considered, the outcomes reached, and details of the outcomes consistent with the continuing protection of confidentiality. The Confidentiality Commission shall also report on its general operations, as well as on its effectiveness and efficiency, and may make proposals or recommendations for its improvement.

Responsibilities of Confidentiality Commission members

2.15 The Confidentiality Commission, and its members individually, shall act without interference or direction from either the Secretariat or other organs of the Organisation, but must follow any mandate of the Conference. The Chair may, however, seek and receive conference and logistical support and assistance from the Secretariat in the exercise of his functions. Confidentiality Commission members with a conflict of interest in relation to a particular dispute shall refrain from dealing with that dispute; it is the responsibility of individual Confidentiality Commission members to declare any conflict of interest as soon as any dispute is notified.

Confidentiality Commission members shall neither exercise any other office within the Organisation or its organs, nor maintain any legal or financial relationship or interest linked to the Organisation.

Meetings of the Confidentiality Commission

2.16 The Confidentiality Commission shall meet initially and in conjunction with regular sessions of the Conference in accordance with paragraph 2.4 of this Part, and shall also meet as necessary to consider disputes brought before it.

2.17 At its initial and subsequent annual meetings, the Confidentiality Commission shall:

(a) choose by consensus a Chair to serve for the forthcoming year taking into account the principle of rotation among the regions designated in paragraph 23 of Article VIII of the Convention;

(b) consider and adopt a report to the Conference as to the outcome of disputes handled by the Confidentiality Commission during the previous year;

(c) consider and adopt a report to the Conference on the operation, effectiveness and efficiency of the Confidentiality Commission and consider any recommendations or proposals made by the Chair in this regard;

(d) as necessary, review and recommend any amendment to its operating procedures;

(e) issue such guidelines to or make such requests of the Chair as it sees fit; and

(f) make such further recommendations or proposals to the Conference as it sees fit.

Preparation of operating procedures

2.18 The Conference shall approve detailed operating procedures for the Confidentiality Commission, setting out, inter alia:

(a) by what formal process meetings of the Confidentiality Commission are to be convened;

(b) how disputes are to be immediately forwarded to the Chair, and how the Chair is to inform all Confidentiality Commission members immediately;

(c) how the Confidentiality Commission is to decide on the timing and process of dispute resolution in accordance with paragraph 2.7 of this Part;

(d) how the Confidentiality Commission is to certify a mutually agreed resolution of a dispute, and how the agreement of disputing parties to such resolution of a dispute is to be registered;

(e) procedures for preparation and submission of reports and recommendations by the Confidentiality Commission to disputing parties and to the Conference or

to another organ of the Organisation in accordance with the Conference's authority;

(f) a procedure to ensure that confidentiality remains protected in the exercise by the Confidentiality Commission of its functions, consistent with the Confidentiality Annex, the OPOC and the need-to-know principle governing access to confidential information;

(g) a procedure for the imposition of time-limits within which Confidentiality Commission functions must be exercised;

(h) procedures for the election of successive Chairs, for the election of successive members to the Confidentiality Commission, and for the filling of any casual vacancies taking into account the principles established in paragraphs 2.1, 2.2, and 2.3 of this Part;

(i) in respect of those Confidentiality Commission members currently considering a particular dispute, a mechanism for facilitating continuity of their service throughout the dispute resolution process, consistent with and subordinate to the principles of the rules governing composition set out in paragraphs 2.1 to 2.4 of this Part;

(j) a procedure by which the Confidentiality Commission's efficiency shall be monitored; and

(k) a procedure for amendment of these operating procedures.

Decision-making procedure

2.19 The Chair shall seek consensus on any decision or recommendation before the Confidentiality Commission as a whole but, in the event that consensus cannot be reached on a particular decision, the Confidentiality Commission may resolve the matter by two-thirds majority of all its members.

3. The role of States Parties in relation to breach procedures

Introduction: relevant Convention obligations

3.1 Provisions of the Convention which specifically relate to States Parties' involvement in the protection of confidentiality include the obligations on individual States Parties to:

(a) to the extent possible, cooperate with and support the Director-General in investigating any breach or alleged breach of confidentiality and in taking appropriate action in case a breach has been established (Confidentiality Annex, paragraph 21);

(b) treat as confidential and afford special handling to information and data received in confidence from the Organisation in connection with the implementation of the Convention, and to treat such information and data

exclusively in connection with rights and obligations under the Convention, and in accordance with the provisions of the Confidentiality Annex (Article VII(6));

(c) treat information received from the Organisation in accordance with the level of confidentiality established for it (Confidentiality Annex, paragraph 4); and

(d) provide upon request details on the handling of confidential information provided to them by the Organisation, including the names of individuals to whom the confidential information has been provided (Confidentiality Annex, paragraph 4).

3.2 In addition, implementation of the provision for waiver of immunity established in paragraph 20 of the Confidentiality Annex would mean that a relevant national jurisdiction would need to apply in the event that a Secretariat staff member committed a serious breach of confidentiality.

3.3 As this Policy deals with the operations of the Organisation itself and its relationship with States Parties, this Part does not establish or prescribe specific internal State Party measures that may be undertaken in pursuance of the objectives of the Convention in relation to confidentiality, or for the implementation of specific States Parties' responsibilities in this regard such as the application of national jurisdiction or the provision of compensation in the event of a breach. If necessary or desirable in particular cases, such specific internal State Party measures or specific responsibilities of States Parties might also be referred to and further developed in bilateral agreements or other implementation arrangements between the Organisation and States Parties.

Possible scenarios

3.4 A State Party's obligations concerning confidentiality could arise in a number of practical scenarios, in particular in relation to:

(a) an OPCW investigation into a breach or alleged breach of confidentiality;

(b) the waiver of immunity by the OPCW Director-General in the event of a serious breach of confidentiality;

(c) a breach of confidentiality for which a State Party is directly responsible; or

(d) a breach of confidentiality by a legal or natural person in the jurisdiction of a State Party.

Investigation of breaches of confidentiality

3.5 In addition to the general requirement under Article VII, paragraph 7 of the Convention to provide assistance to the Secretariat, each State Party has a particular obligation in relation to the investigation by the Director-General of a breach or alleged breach of confidentiality (as noted in subparagraph 3.1(a) of this Part). Within the framework of these obligations, the nature of support and cooperation by States

Parties in relation to any particular investigation is to be determined on a case-by-case basis.

Waiver of immunity in the case of a serious breach of confidentiality

3.6 The Convention (Confidentiality Annex, paragraphs 20 and 21) presumes that jurisdiction should apply in the event of immunity from jurisdiction being waived in respect of a staff member of the Technical Secretariat who has committed a serious breach of confidentiality. If the Director-General decides to waive immunity in such a case, legal proceedings under an applicable jurisdiction of a State Party should be instituted against such a staff member on the basis of the request of the Director-General or a State Party affected by the serious breach. States Parties should take any appropriate administrative and legal measures to ensure that this mechanism can be effectively implemented.

3.7 It will remain the primary responsibility of States Parties to determine the applicability of national jurisdiction on a case-by-case basis. The Conference may also consider proposals for an arrangement that would ensure a consistent and comprehensive response to any serious breach of confidentiality obligations by Secretariat staff members.

Breaches imputed to a State Party

3.8 If information provided in confidence by the Organisation to a State Party is disclosed to unauthorised recipients or if confidentiality is otherwise abused by that State Party, then this would run contrary to the obligations upon States Parties established under Article VII, paragraph 6 of the Convention and under the Confidentiality Annex, paragraph 4. Treatment as confidential of information received in confidence is, moreover, an essential part of the effective operation of the Convention as a whole. In such a case, a breach of confidentiality may be imputed to the State Party in question, as contravening these obligations. This may arise as a finding of an investigation by the Director-General into a breach or alleged breach,[16] in which case the matter would be subject to the Convention's dispute resolution mechanisms, and in particular to the Confidentiality Commission[17] under the authority of the Conference.

Other application of national jurisdiction

3.9 As noted in paragraph 3.8 above, a State Party's disclosure of information, having been provided by the Organisation in confidence, in such a way as to breach its confidentiality would run contrary to the obligations upon States Parties established under Article VII, paragraph 6 of the Convention and under the Confidentiality Annex, paragraph 4. States Parties are therefore required to take appropriate administrative and legal measures they judge to be necessary to ensure that these obligations are effectively met, including by any agents acting with their authority or sponsorship.

---

16 In accordance with Step 4e of the breach investigation procedures in section 1.

17 See section 2.

PART X

ANNUAL REPORT ON THE IMPLEMENTATION OF THE REGIME GOVERNING THE HANDLING OF CONFIDENTIAL INFORMATION BY THE SECRETARIAT

1. The Director-General is required to report annually to the Conference on the implementation of the regime governing the handling of confidential information by the Secretariat (Confidentiality Annex, paragraph 3). The points identified below should be covered in the report, but in such a way as to preclude any diminution of the confidentiality of any confidential information disclosed to, handled by or held in the Secretariat, and governed by the principles of this Policy.

2. The Director-General shall focus in his report on practical details of the handling of confidential information by staff members of the Secretariat (CA, paragraph 3) in the preceding year, including:

   (a) resource requirements for implementing the confidentiality regime, including an estimate of the volume of confidential information handled by the Secretariat;

   (b) important actions taken to implement the confidentiality regime, including significant changes in procedures or personnel, and staff training and awareness programmes to ensure compliance of Secretariat staff with the regime;

   (c) breaches or alleged breaches and the actions taken to investigate and redress them; and

   (d) problems or policy issues that have arisen with respect to the confidentiality regime.

3. While not limiting the scope of the report, it should in particular cover the following detailed elements:

   (a) the estimated number of items of confidential information received, generated, stored and disseminated by the Secretariat;

   (b) the number, recipients and description of release[18] of items of confidential information made during the previous year, and access granted to authorised recipients associated with the Organisation;[19]

---

[18] "Release" of information refers to the approved disclosure of information beyond the Organisation itself (including all its constituent elements) and beyond the governments of States Parties (specifically, beyond governmental organisations and authorised entities or individuals within States Parties concerned with the operation of the Convention (paragraph 1.1 of Part VII of this Policy)).

[19] In accordance with the principles set out in section 6 of Part VI of this Policy.

(c) the number of clearances granted for access to confidential information in accordance with paragraph 11 of the Confidentiality Annex, and any changes in senior staff positions concerned with the implementation of the confidentiality regime;

(d) resource and operational requirements and general policy issues arising from confidentiality procedures in the course of verification activities and in the IMS;

(e) any changes that have been made in administrative directives established to implement this Policy, including any changes to administrative directives that have been made necessary by the Conference's approval of amendments to this Policy;

(f) any reported loss of confidential information;

(g) any breaches or alleged breaches involving staff members of the Secretariat, breach investigations conducted by the Director-General, and consequent actions taken;

(h) any changes in the IMS which have substantial implications for the security of confidential information contained in the system;

(i) the conduct of staff training and awareness programmes about the obligation to protect confidential information and to abide by the confidentiality regime, and the provision of instruction, advice and regular reminders to all staff members of the Secretariat about the principles of this Policy and the procedures required to implement it, as well as about the principles and procedures relating to security, and the possible penalties that staff members would incur in the event of improper disclosure of confidential information; and

(j) the number of items of confidential information to which authorised recipients associated with the Organisation were granted access in accordance with the principles set out in section 6 of Part VI of this Policy.

PART XI

AMENDMENT PROCEDURE

1. Any State Party or the Director-General may propose amendments to this Policy. Any proposed amendments shall be forwarded by the Director-General, through the Executive Council, to the Conference of the States Parties for its consideration and approval in accordance with its rules of procedure.

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 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.

GLOSSARY

‘The Convention’: The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction

‘The Confidentiality Annex’ or ‘CA’: The Annex on the Protection of Confidential Information, annexed to the Convention

‘The Organisation’ or ‘The OPCW’: The Organisation for the Prohibition of Chemical Weapons, established under Article VIII, paragraph 1, of the Convention

‘The Conference’: The Conference of the States Parties established under Article VIII, paragraph 4 of the Convention

‘The Secretariat’: The Technical Secretariat established under Article VIII, paragraph 4 of the Convention

‘The Confidentiality Commission’: The Commission for the settlement of disputes related to confidentiality cited in paragraph 23 of the Confidentiality Annex

‘MCP’: Manual of Confidentiality Procedure

‘OCS’: Office of Confidentiality and Security in the Technical Secretariat

‘IMS’: Information Management System

- - - o - - -