OPCW **Conference of the States Parties**

Twenty-Second Session C-22/DEC.15
27 November – 1 December 2017 30 November 2017
Original: ENGLISH

DECISION

AMENDMENTS TO THE OPCW POLICY ON CONFIDENTIALITY

The Conference of the States Parties,

Recalling its decision adopting the OPCW Policy on Confidentiality (OPOC) (C-I/DEC.13/Rev.1, dated 2 February 2006);

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

Recalling further that the Director-General, in response to the recommendations from the OPCW's Office of Confidentiality and Security, convened a confidentiality reform task force (CRTF) to provide advice to the OPCW on any necessary modifications to the OPCW confidentiality regime;

Noting that the report of the Director-General on the OPCW confidentiality regime (EC-85/DG.22 C-22/DG.6, dated 23 June 2017) refers to the recommendation of the CRTF that the OPOC be amended in line with established practices and advances in information technology; and

Noting also the recommendation of the Council on this matter at its Eighty-Fifth Session (EC-85/DEC.6, dated 12 July 2017);

Hereby:

Adopts the amendments to the OPOC annexed hereto.

Annex: Amendments to the OPCW Policy on Confidentiality

Annex

AMENDMENTS TO THE OPCW POLICY ON CONFIDENTIALITY

	Reference	Existing text	Justification for Amendment	Proposed text
1.	Part I, paragraph 1	This document sets out the basis of 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.	The OPOC is too comprehensive to be considered a “basis.”	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.	Part II, subparagraph 3(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 an inspected 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;	Contingency operations require that these rights are conferred on all States Parties as activities which are not considered inspections can take place.	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;
3.	Part II, subparagraph 3(d)	systematic procedures for limiting the dissemination of and access to information after information is collected and classified as confidential shall be established, monitored, and adhered to;	Phrasing altered to clarify that this applies to confidential information.	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;
4.	Part II, subparagraph 3(f)	staff selection and training, and staffing policy and regulations, shall take into account the need to ensure that all staff members of the Secretariat meet the highest standards of efficiency, competence and integrity.	There are many references to “staff members” in the OPOC. Rather than correcting all of them (resulting in a large number of changes) it would be	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

	Reference	Existing text	Justification for Amendment	Proposed text
			better to have one statement clarifying that this decision applies to all of the employment relationships that the OPCW may be involved in.	highest standards of efficiency, competence and integrity.
5.	Part III, paragraph 8	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: - '**Document**' could extend to a variety of physical items displaying information or data; - '**Computer material**' includes any computer storage and processing medium, such as disks, tapes and diskettes. This term also covers portable computers, which may be used to record information during an on-site inspection; - '**Audio-visual material**' includes audio and video tapes, developed and undeveloped photographic films including the negatives of still photographs and the positives. (Positive prints of still photographs may be considered also as documents); and - '**Sample**' includes a sample's collection medium and any further information acquired or derived from analysis.	These terms have been updated to reflect the modern technological environment.	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: - '**Document**' could extend to a variety of physical items displaying information or data; - '**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*; - '**Audio-visual material**' includes audio and video *recordings and digital images*; - '**Sample**' includes a sample's collection medium and any further information acquired or derived from analysis. In the application of general operating guidelines to particular items of information falling under

	Reference	Existing text	Justification for Amendment	Proposed text
		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).		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).
6.	Part IV, paragraph 1.3.1	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 in pursuance of CWC obligations, as well as sensitive information not relevant to the aims of the Convention in the event that such sensitive information is disclosed.	Minor change to streamline phrasing.	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.
7.	Part IV, subparagraph 1.3.2(a)	through the appropriate unit, to evaluate all data and documents it obtains to determine whether confidential information is included;	Minor change to clarify that this refers to a formal administrative division.	through the appropriate *organisational* unit, to evaluate all *information* it obtains to determine whether confidential information is included;

	Reference	Existing text	Justification for Amendment	Proposed text
8.	Part IV, subparagraph 1.4.2(c)	fully respect the procedures designed to protect sensitive installations and to prevent the unauthorised disclosure of confidential data;	Modified to clarify the obligation.	fully respect the procedures designed to protect sensitive installations and to prevent the unauthorised disclosure of confidential *information*;
9.	Part IV, paragraph 2.1.5		Changed to reflect current practice.	*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.*
10.	Part V, paragraph 1.8	Unless specified otherwise, due to the greater or lesser sensitivity of the data in question, the following forms of information might be classified **OPCW RESTRICTED** when they are acquired or generated by any means by the Organisation:	Changed to reflect current practice.	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:
11.	Part V, paragraph 1.12	Unless specified otherwise in accordance with greater or lesser sensitivity, the following forms of information might be classified as **OPCW PROTECTED** when they are acquired or generated by any means by the Organisation:	Changed to reflect current practice.	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:
12.	Part V, subparagraph 1.12(e)	data and information regarding inspection planning of the Secretariat and the inspection goals for a specific facility;	Changed to reflect current practice.	data and information regarding inspection planning of the Secretariat, the inspection goals for a specific facility *and travel arrangements*;
13.	Part V, subparagraph 1.12(f)	facility agreements and any attachments thereto; and	Changed to reflect current practice.	facility agreements and any attachments thereto;

	Reference	Existing text	Justification for Amendment	Proposed text
14.	Part V, subparagraph 1.12(g)	information regarding the validation and evaluation of information contained in declarations, facility agreements and inspection reports.	Minor correction.	information regarding the validation and evaluation of information contained in declarations, facility agreements and inspection reports; *and*
15.	Part V, paragraph 1.15	Unless specified otherwise in accordance with lesser sensitivity, the following forms of information might be classified as **OPCW HIGHLY PROTECTED** when they are acquired or generated by any means by the Organisation:	Changed to reflect current practice.	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:
16.	Part V, paragraph 1.17	Sensitive confidential 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 subparagraph 2.5 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.	The term confidential has been removed to avoid confusion since this paragraph mandates the treatment of non-classified information as though it *were* classified.	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 2.5 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.

	Reference	Existing text	Justification for Amendment	Proposed text
17.	Part V, paragraph 2.1	For information which has been determined to be classified 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 will include an internal procedure for maintaining consistency of classification for documents generated within the Secretariat, and for consulting on and, if necessary, authorising such classification.	Modified to correct a probable drafting error.	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.
18.	Part V, subparagraph 2.2(a)	in the case of confidential information provided by a State Party, that State Party has the authority to designate its initial classification category; - if a State Party provides information which appears to be confidential without indicating a level of sensitivity, 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	Modified to clarify the involved procedure as the OPOC does not have "sensitivity levels."	in the case of confidential information provided by a State Party, that State Party has the authority to designate its classification category; - 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

	Reference	Existing text	Justification for Amendment	Proposed text
19.	Part V, paragraph 2.5	**Classification authority in the course of inspections** During the course of an inspection, or in the formulation of a facility agreement, an inspected State Party 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 and in the transmission of confidential information to the Secretariat on completion of the inspection. In cases when the inspected State Party discloses to any member of the inspection team sensitive confidential information without establishing a formal classification for it, or when such information is revealed to any member of the inspection team, this member will bear the responsibility of treating this information as **OPCW HIGHLY PROTECTED**, unless the inspected State Party specifies otherwise.	Changed to reflect current practice.	**Classification authority in the course of inspections *or other operational deployments*** 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.
20.	Part VI, paragraph 1.2	These principles are to be applied in the detailed elaboration of all procedures relating to the handling of confidential information, including in the OPCW Inspection Manual, the Declaration Handbook, and the Manual of Confidentiality Procedure (MCP). Further practical procedures shall be set out on the basis of these principles in	Changed to reflect current practice.	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

	Reference	Existing text	Justification for Amendment	Proposed text
		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.		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.
21.	Part VI, paragraph 3.10	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: - documents, including papers and paper files; - computer material; - audio-visual material; and - samples.	Modified to reflect changes in information technology.	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: - *hard-copy* documents, including papers and paper files; - *information in electronic or magnetic form;* - computer *equipment and systems*;

	Reference	Existing text	Justification for Amendment	Proposed text
		These administrative directives shall aim at establishing practical mechanisms for ensuring that all the principles established in this document are met.		- audio-visual material; and - samples. These administrative directives shall aim at establishing practical mechanisms for ensuring that all the principles established in this document are met.
22.	Part VI, paragraph 4.1	In order to ensure the proper handling of OPCW confidential information, all documents and media for information storage shall be clearly marked in accordance with the marking instructions set out in an administrative directive issued by the Director-General and supervised by the OCS. 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: - **OPCW RESTRICTED** - **OPCW PROTECTED** - **OPCW HIGHLY PROTECTED**	Changed to reflect current practice.	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: - **OPCW RESTRICTED** - **OPCW PROTECTED** - **OPCW HIGHLY PROTECTED**
23.	Part VI, paragraph 4.12	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: - guidelines for secure mailing or manual	Modified to reflect changes in information technology.	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: - guidelines for secure mailing or manual

	Reference	Existing text	Justification for Amendment	Proposed text
		transmission, and the safe-hand carriage, of confidential information; and - procedures for secure transmission by telephone, telefacsimile and other telecommunications systems.		transmission, and the safe-hand carriage, of confidential information; and - procedures for secure transmission by telephone, telefacsimile, *email, file transfer* and other telecommunications systems *or methods.*
24.	Part VI, paragraph 4.17	The Director-General shall set out, in an administrative directive, physical security measures for offices, laboratories, information storage 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, and the OPCW Laboratory.	Modifications reflect changes in technology as well as current practice.	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.
25.	Part VI, paragraph 4.20	Handling procedures shall be established in an administrative directive issued by the Director-General to cover the carriage of confidential information from the premises of the Organisation, between inspected sites and the Organisation, and	Changed to reflect updates in information technology as well as to provide for its application to activities apart from inspections.	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*

	Reference	Existing text	Justification for Amendment	Proposed text
		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.		*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.
26.	Part VI, paragraph 4.21	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, 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.	Changed to reflect updates in information technology as well as to provide for its application to activities apart from inspections.	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.
27.	Part VI, paragraph 5.3	Access to all sites of the OPCW and key components of the IMS, such as the servers and mass storage devices, must be controlled. All hardware in the confidential part of the IMS, and especially workstations, servers and user terminals shall be protected, not only from theft or criminal damage, but also from unauthorised physical access and tampering attempts. In addition, maintenance and repair activities on confidential IMS hardware shall be supervised and recorded. Access to such hardware items as servers, printers, back-up	Changed to reflect updates in information technology and to reflect current practice in the Technical Secretariat.	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*

	Reference	Existing text	Justification for Amendment	Proposed text
		devices, as well as other output devices, shall be limited to staff members with appropriate clearances.		*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.
28.	Part VI, paragraph 5.5	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 security management and operations.	Changed to reflect updates in information technology as well as to provide for its application to activities apart from inspections.	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.
29.	Part VI, paragraph 5.6	Computer material (including portable storage media such as diskettes) and confidential information stored in the OPCW IMS 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.	Changed to reflect current practice.	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.
30.	Part VI, paragraph 5.8	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	Changed to reflect current practice.	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

	Reference	Existing text	Justification for Amendment	Proposed text
		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 inspected 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.		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.
31.	Part VI, paragraph 6	**Handling and protection of confidential information during on-site verification activities**	Changed to reflect current practice.	**Handling and protection of confidential information *during operational deployments***
32.	Part VI, paragraph 6.1		Insertion of new paragraph to indicate that the procedures described in paragraph 6 covers any operational deployment	*All references to inspections, inspection teams, inspectors, and inspected States Parties in paragraph 6 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*

	Reference	Existing text	Justification for Amendment	Proposed text
33.	Part VI, paragraphs 6.1 to 6.3	**6.1** **6.2** **6.3**	Renumbering of paragraphs	**6.2** **6.3** **6.4**
34.	Part VI, paragraph 6.4	**On-site verification: protection of non-relevant confidential information.**	Title of section changed for clarification.	**Protection of non-relevant confidential information**
35.		**6.5** **6.6** **6.7** **6.8**	Renumbering of paragraphs	**6.6** **6.7** **6.8** **6.9**
36.	Part IX.1, subparagraph 3.1(a)	following 'sufficient indication' that there has been a violation of an obligation to protect confidential information on the part of a staff member of the Secretariat, another authorised individual or entity beyond the Secretariat , or an agent or official of a State Party; or	Footnote has been added to clarify the meaning of “sufficient indication” in this context.	following 'sufficient indication' 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 *Footnote: 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.*

	Reference	Existing text	Justification for Amendment	Proposed text
37.	Part IX.1, paragraph 3.4	When a decision has been taken by the Director-General to proceed with an investigation, the decision should be made known immediately to any States Parties and any Secretariat staff member involved in the alleged breach or suspected violation.	Changed to give extra guidance for the procedure outlined.	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.
38.	Part IX.1, paragraph 3.6	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 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.	Footnote has been added to clarify the meaning of “prima facie” in this context.	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 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. *Footnote: 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.*

	Reference	Existing text	Justification for Amendment	Proposed text
39.	Part IX.1, subparagraph 4.1(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 or denial of access to certain information, or, if the case appears serious, temporary suspension in accordance with the OPCW Staff Regulations and Rules;	Clarified to empower the Director-General to freeze funds controlled by the OPCW.	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;
40.	Part IX.1, paragraph 4.2	An employee 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.	Changed for consistency.	*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.
41.	Part IX.1, paragraph 4.5		This change clarifies the Director-General's abilities during the course of an investigation.	*The Director-General is empowered to take the interim actions set forth in this section at any time from the establishment of a <u>prima facie</u> case until the conclusion of the investigation.*
42.	Part IX.1, paragraph 5.5	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. 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 can not 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	This has been changed to prevent investigators from being required to inform the investigation subjects of the progress of the investigation.	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

	Reference	Existing text	Justification for Amendment	Proposed text
		accordance with paragraph 23 of the Confidentiality Annex.		and in his report request that the Confidentiality Commission be convened to consider the case in accordance with paragraph 23 of the Confidentiality Annex.
43.	Part IX.1, paragraph 8	**Step 4b: Sanctions against former Secretariat staff** If a breach or violation is determined within the report to have been committed by a former member of staff of the Secretariat, the Director-General may decide on the application of whatever measures may still be applied within the terms of the OPCW Staff Regulations and Rules. This may include the loss of financial or other entitlements, such as those related to the OPCW Provident Fund.	This section has been amended to provide clarity for actions which may be taken in relation to former staff members.	**Step 4b: Sanctions against former Secretariat staff** If a breach or violation is determined within the report to have been committed by a former member of staff of the Secretariat, the Director-General may decide on the application of *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.* *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.*

	Reference	Existing text	Justification for Amendment	Proposed text
44.	Part IX.3, subparagraph 1.1(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 (paragraph 21, Confidentiality Annex);	Changed to reflect current practice.	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*);
45.	Part IX.3, subparagraph 1.1(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);	Changed to reflect current practice.	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)*);
46.	Part IX.3, subparagraph 1.1(d)	provide upon request details on the handling of confidential information provided to them by the Organisation (Confidentiality Annex, paragraph 4).	This change will facilitate investigations of breaches involving States Parties.	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).

- - - o - - -