RULES GOVERNING THE TREATMENT OF CONFIDENTIAL INFORMATION BY THE EUROPEAN PARLIAMENT

BUREAU DECISION

OF 15 APRIL 2013[1]

HE BUREAU OF THE EUROPEAN PARLIAMENT,

Having regard to Rule 23(12) of the Rules of Procedure of the European Parliament,

Whereas:

(1) In the light of the Framework Agreement on relations between the European Parliament and the European Commission[2] signed on 20 October 2010 ('the Framework Agreement') and the Interinstitutional Agreement between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters other than those in the area of the Common Foreign and Security Policy[3] signed on 12 March 2014 ('the Interinstitutional Agreement'), it is necessary to lay down specific rules on the treatment of confidential information by the European Parliament.

(2) The Lisbon Treaty assigns new tasks to the European Parliament and, in order to develop Parliament's activities in those areas which require a degree of confidentiality, it is necessary to lay down basic principles, minimum standards of security and appropriate procedures for the treatment by the European Parliament of confidential, including classified, information.

(3) The rules laid down in this Decision aim at ensuring equivalent standards of protection and compatibility with the rules adopted by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States, in order to facilitate the smooth functioning of the decision-making process of the European Union.

(4) The provisions of this Decision are without prejudice to current and future rules on access to documents adopted in accordance with Article 15 of the Treaty on the Functioning of the European Union (TFEU).

(5) The provisions of this Decision are without prejudice to current and future rules on the protection of personal data adopted in accordance with Article 16 TFEU,

---

1 OJ C 96, 1.4.2014, p. 1.
2 OJ L 304, 20.11.2010, p. 47.
3 OJ C 95, 1.4.2014, p. 1.

7.3.3.

HAS ADOPTED THIS DECISION:

Article 1

Objective

This Decision governs the management and handling of confidential information by the European Parliament, including the creation, reception, forwarding and storage of such information, with a view to the appropriate protection of its confidential nature. It implements, the Interinstitutional Agreement and the Framework Agreement, in particular Annex II thereto.

Article 2

Definitions

For the purposes of this Decision:

(a)‘information’ means any written or oral information, whatever the medium and whoever the author may be;

(b)‘confidential information’ means ‘classified information’, and non-classified ‘other confidential information’;

(c)‘classified information’ means ‘EU classified information’ and ‘equivalent classified information’;

(d)‘EU classified information’ (EUCI) means any information and material, classified as ‘TRÈS SECRET UE/EU TOP SECRET’, ‘SECRET UE/EU SECRET’, ‘CONFIDENTIEL UE/EU CONFIDENTIAL’ or ‘RESTREINT UE/EU RESTRICTED’, unauthorised disclosure of which could cause varying degrees of prejudice to Union interests or to those of one or more of its Member States, whether or not such information originates within the institutions, bodies, offices or agencies established by virtue or on the basis of the Treaties. In this regard, information and material classified at the level:

– ‘TRÈS SECRET UE/EU TOP SECRET’ is information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the Union or of one or more of the Member States;

– ‘SECRET UE/EU SECRET’ is information and material the unauthorised disclosure of which could seriously harm the essential interests of the Union or of one or more of the Member States;

– ‘CONFIDENTIEL UE/EU CONFIDENTIAL’ is information and material the unauthorised disclosure of which could harm the essential interests of the Union or of one or more of the Member States;

– ‘RESTREINT UE/EU RESTRICTED’ is information and material the unauthorised disclosure of which could be disadvantageous to the interests of the Union or of one or more of the Member States;

(e)‘equivalent classified information’ means classified information issued by Member States, third States or international organisations which bears a security classification marking equivalent to one of the security classification markings used for EUCI and which has been forwarded to the European Parliament by the Council or the Commission;

7.3.3.

(f)‘other confidential information’ means any other non-classified confidential information, including information covered by data protection rules or by the obligation of professional secrecy, created in the European Parliament or forwarded to the European Parliament by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States;

(g)‘document’ means any recorded information, regardless of its physical form or characteristics;

(h)‘material’ means any document or item of machinery or equipment, either manufactured or in the process of manufacture;

(i)‘need to know’ means the need of a person to have access to confidential information in order to be able to perform an official function or a task;

(j)‘authorisation’ means a decision adopted by the President, if it concerns Members of the European Parliament, or by the Secretary-General, if it concerns officials of the European Parliament and other European Parliament employees working for political groups, to grant an individual access to classified information up to a specific level, on the basis of a positive result of a security screening (vetting) carried out by a national authority under national law and pursuant to the provisions laid down in Annex I, Part 2;

(k)‘downgrading’ means a reduction in the level of classification;

(l)‘declassification’ means the removal of any classification;

(m)‘marking’ means a sign affixed to ‘other confidential information’ intended to identify predefined specific instructions about its handling or the field covered by a given document. It may also be affixed to classified information, in order to impose additional requirements for its handling;

(n)‘unmarking’ means the removal of any marking;

(o)‘originator’ means the duly authorised author of confidential information;

(p)‘security notices’ means the implementing measures laid down in Annex II;

(q)‘handling instructions’ means technical instructions issued to the European Parliament's services concerning the management of confidential information.

Article 3

Basic principles and minimum standards

1. The treatment of confidential information by the European Parliament shall follow the basic principles and minimum standards laid down in Annex I, Part 1.

2. The European Parliament shall set up an information security management system (ISMS) in accordance with those basic principles and minimum standards. The ISMS shall consist of the security notices, the handling instructions and the relevant Rules of Procedure. It shall aim at facilitating parliamentary and administrative work, while ensuring the protection of any confidential information processed by the European Parliament, in full respect of the rules established by the originator of such information as laid down in the security notices.

The processing of confidential information by means of automated communication and information systems (CIS) of the European Parliament shall be implemented in accordance with the concept of information assurance (IA), as provided for in security notice 3.

3. Members of the European Parliament may consult classified information up to and including the level RESTREINT UE/EU RESTRICTED without security clearance.

4. Where the information concerned is classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent, access shall be granted to those Members of the European Parliament who have been authorised by the President pursuant to paragraph 5 or after having signed a solemn declaration of non-disclosure of the content of that information to third persons, of compliance with the obligation to protect information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL and of acknowledgement of the consequences of any failure to do so.

5. Where the information concerned is classified at the level SECRET UE/EU SECRET or TRÈS SECRET/EU TOP SECRET or its equivalent, access shall be granted to those Members of the European Parliament who are authorised by the President after:

(a) they have been security-cleared in accordance with Annex I, Part 2, of this Decision, or

(b) a notification has been received from a competent national authority that the Members concerned are duly authorised by virtue of their functions in accordance with national law.

6. Before being granted access to classified information, Members of the European Parliament shall be briefed on, and shall acknowledge, their responsibilities regarding the protection of such information in accordance with Annex I. They shall also be briefed on the means of ensuring such protection.

7. Officials of the European Parliament and other European Parliament employees working for political groups may consult confidential information if they have an established 'need to know', and may consult classified information above the level RESTREINT UE/EU RESTRICTED if they hold the appropriate level of security clearance. Access to classified information shall be granted only if they have been briefed on, and received written instructions concerning, their responsibilities regarding the protection of such information, as well as the means of ensuring such protection, and if they have signed a declaration acknowledging receipt of those instructions and undertaking to comply with them in accordance with the current rules.

Article 4

Creation of confidential information and administrative handling by the European Parliament

1. The President of the European Parliament, the chairs of the parliamentary committees concerned and the Secretary-General and/or any person duly authorised by him/her in writing may originate confidential information and/or classify information as provided for in the security notices.

2. When creating classified information, the originator shall apply the appropriate level of classification in line with the international standards and definitions set out in Annex I. The originator shall also determine, as a general rule, the addressees who are to be authorised to consult the information commensurate to the level of classification. This information shall be communicated to the Classified Information Unit (CIU) when the document is deposited with the CIU.

3. 'Other confidential information' covered by professional secrecy shall be dealt with in accordance with Annexes I and II and the handling instructions.

Article 5

Reception of confidential information by the European Parliament

1. Confidential information received by the European Parliament shall be communicated as follows:

(a) information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information': to the secretariat of the parliamentary body/office-holder which submitted the request therefor, or directly to the CIU;

(b) information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent: to the CIU.

2. The registration, storage and traceability of confidential information shall be dealt with, as the case may be, either by the secretariat of the parliamentary body/office-holder who received the information or by the CIU.

3. The agreed arrangements to be established by common accord with a view to preserving the confidentiality of the information, in the case of confidential information communicated by the Commission pursuant to point 3.2 of Annex II to the Framework Agreement, or in the case of classified information forwarded by the Council pursuant to Article 5(4) of the Interinstitutional Agreement, shall be deposited, together with the confidential information, at the secretariat of the parliamentary body/office-holder or at the CIU, as the case may be.

4. The arrangements referred to in paragraph 3 may also be applied mutatis mutandis for the communication of confidential information by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States.

5. In order to ensure a level of protection commensurate with the level of classification TRÈS SECRET UE/EU TOP SECRET or its equivalent, the Conference of Presidents shall set up an oversight committee. Information classified at the level TRÈS SECRET UE/EU TOP SECRET or its equivalent shall be communicated to the European Parliament subject to further arrangements, to be agreed between the European Parliament and the Union Institution from whom the information is received.

Article 6

Communication of classified information by the European Parliament to third parties

The European Parliament may, subject to the prior written consent of the originator or the Union Institution, which has communicated the classified information to the European Parliament, as the case may be, forward such classified information to third parties, on condition that they ensure that, when such information is handled, rules equivalent to those laid down in this Decision are respected within their services and premises.

Article 7

Secure facilities

1. For the purposes of the management of confidential information, the European Parliament shall establish a Secure Area and Secure Reading Rooms.

2. The Secure Area shall provide facilities for the registration, consultation, archiving, transmission and handling of classified information. It shall comprise, inter alia, a reading

room and a meeting room for the consultation of classified information and shall be managed by the CIU.

3. Outside the Secure Area, Secure Reading Rooms may be created, in order to allow for the consultation of information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent, and of 'other confidential information'. Those Secure Reading Rooms shall be managed by the competent services of the secretariat of the parliamentary body/office-holder or by the CIU, as the case may be. They shall not contain photocopying machines, telephones, fax facilities, scanners or any other technical equipment for the reproduction or transmission of documents.

Article 8

Registration, handling and storage of confidential information

1. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' shall be registered and stored by the competent services of the secretariat of the parliamentary body/office-holder or by the CIU, depending on who received the information.

2. The following conditions shall apply to the handling of information classified at the level RESTREINT EU/EU RESTRICTED or its equivalent and 'other confidential information':

(a) documents shall be handed over in person to the head of the secretariat, who shall register them and provide an acknowledgement of receipt;

(b) when not actually being used, such documents shall be kept in a locked location, under the responsibility of the secretariat;

(c) in no case may the information be saved on another medium or transmitted to any person. Such documents may only be duplicated by means of appropriately accredited equipment as defined in the security notices;

(d) access to such information shall be restricted to those designated by the originator or by the Union Institution which communicated the information to the European Parliament, in accordance with the arrangements referred to in Article 4(2) or Article 5(3), (4) and (5);

(e) the secretariat of the parliamentary body/office-holder shall keep a record of the persons who have consulted the information, and of the date and time of such consultation, and shall transmit the record to the CIU at the time when the information is deposited with the CIU.

3. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall be registered, handled and stored by the CIU in the Secure Area, in accordance with the specific level of classification and as defined in the security notices.

4. In the event of a breach of the rules set out in paragraghs 1 to 3, the responsible official of the secretariat of the parliamentary body/office-holder or of the CIU, as the case may be, shall inform the Secretary-General, who shall refer the matter to the President if a Member of the European Parliament is concerned.

Article 9

Access to secure facilities

1. Only the following persons shall have access to the Secure Area:

(a) persons who, pursuant to Article 3(4) to (7), are authorised to consult the information held there and who have submitted an application pursuant to Article 10(1);

(b) persons who, pursuant to Article 4(1), are authorised to create classified information and who have submitted an application pursuant to Article 10(1);

(c) the European Parliament's officials of the CIU;

(d) the European Parliament officials responsible for managing the CIS;

(e) European Parliament officials responsible for security and fire safety, when necessary;

(f) cleaning staff, but only in the presence of, and under close surveillance by, an official of the CIU.

2. The CIU may deny access to the Secure Area to any person not authorised to enter. Any objection challenging such a denial of access shall be submitted to the President, in the case of a request for access by a Member of the European Parliament, and to the Secretary-General in other cases.

3. The Secretary-General may authorise a meeting for a limited number of persons in the meeting room located within the Secure Area.

4. Only the following persons shall have access to a Secure Reading Room:

(a) Members of the European Parliament, officials of the European Parliament and other European Parliament employees working for political groups, duly identified for the purposes of consultation or creation of confidential information;

(b) the European Parliament officials responsible for managing the CIS, officials of the secretariat of the parliamentary body/office-holder which received the information, and officials of the CIU;

(c) where necessary, European Parliament officials responsible for security and fire safety;

(d) cleaning staff, but only in the presence of, and under close surveillance by, an official working in the secretariat of the parliamentary body/office-holder or in the CIU, as the case may be.

5. The competent secretariat of the parliamentary body/office-holder or the CIU, as the case may be, may deny access to a Secure Reading Room to any person not authorised to enter. Any objection challenging such a denial of access shall be submitted to the President, in the case of a request for access by a Member of the European Parliament, and to the Secretary-General in other cases.

Article 10

Consultation or creation of confidential information in secure facilities

1. Any person wishing to consult or create confidential information in the Secure Area shall communicate his or her name in advance to the CIU. The CIU shall check the identity of that person and verify whether he or she is permitted, in accordance with Article 3(3) to (7), Article 4(1) or Article 5(3), (4) and (5) to consult or create confidential information.

2. Any person wishing, in accordance with Article 3(3) and (7), to consult confidential information classified at the level RESTREINT EU/EU RESTRICTED or its equivalent or ‘other confidential information’ in a Secure Reading Room shall communicate his or her

name in advance to the competent services of the secretariat of the parliamentary body/office-holder or to the CIU.

3. Save in exceptional circumstances (e.g. where numerous requests for consultation are submitted within a short period of time), only one person at a time shall be authorised to consult confidential information in a secure facility, in the presence of an official of the secretariat of the parliamentary body/office-holder or of the CIU.

4. During the consultation process, contact with the exterior (including by means of telephones or other technological devices), the taking of notes and the photocopying or photographing of the confidential information consulted shall be prohibited.

5. Before authorising a person to leave the secure facility, the official of the secretariat of the parliamentary body/office-holder or of CIU shall check that the confidential information consulted is still present, intact and complete.

6. In the event of a breach of the rules set out above, the official of the secretariat of the parliamentary body/office-holder or of the CIU shall inform the Secretary-General, who shall refer the matter to the President where a Member of the European Parliament is concerned.

Article 11

Minimum standards for consultation of confidential information at a meeting in camera outside secure facilities

1. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' may be consulted by members of parliamentary committees or of other political and administrative bodies of the European Parliament at a meeting in camera outside the secure facilities.

2. In the circumstances provided for in paragraph 1, the secretariat of the parliamentary body/office-holder responsible for the meeting shall ensure that the following conditions are complied with:

(a) only the persons designated by the chair of the competent committee or body to participate in the meeting are allowed to enter the meeting room;

(b) all documents are numbered, distributed at the beginning of the meeting and collected again at the end, and no notes of those documents and no photocopies or photographs thereof are taken;

(c) the minutes of the meeting make no mention of the content of the discussion of the information considered. Only the relevant decision, if any, may be recorded;

(d) confidential information provided orally to recipients in the European Parliament is subject to a level of protection equivalent to that applied to confidential information in written form;

(e) no additional stock of documents is held in meeting rooms;

(f) copies of documents are distributed only in the requisite numbers to participants and interpreters at the start of the meeting;

(g) the classification/marking status of the documents is made clear by the chair of the meeting at the start of the meeting;

(h) participants do not remove documents from the meeting room;

(i) all copies of documents are collected and accounted for at the end of the meeting by the secretariat of the parliamentary body/office-holder; and

(j) no electronic communication devices or other electronic devices are taken into the meeting room where the confidential information in question is consulted or discussed.

3. Where, in accordance with the exceptions laid down in point 3.2.2 of Annex II to the Framework Agreement and in Article 6(5) of the Interinstitutional Agreement, information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent is discussed at a meeting held in camera, the secretariat of the parliamentary body/office-holder responsible for the meeting shall, in addition to ensuring compliance with the provisions laid down in paragraph 2, ensure that the persons designated to participate in the meeting comply with the requirements of Article 3(4) and (7).

4. In the case provided for in paragraph 3, the CIU shall provide to the secretariat of the parliamentary body/office-holder-responsible for the meeting in camera the requisite number of copies of the documents to be discussed, which shall be returned to the CIU after the meeting.

Article 12

Archiving of confidential information

1. Secure archiving facilities shall be provided within the Secure Area. The CIU shall be responsible for managing the secure archive in accordance with standard archiving criteria.

2. Classified information definitively deposited with the CIU, and information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent which is deposited with the secretariat of the parliamentary body/office-holder, shall be transferred to the secure archive in the Secure Area six months after it was last consulted and, at the latest, one year after it was deposited. 'Other confidential information' shall be archived, unless deposited with the CIU, by the secretariat of the parliamentary body/office-holder concerned, in accordance with the general rules on document management.

3. Confidential information held in the secure archive may be consulted subject to the following conditions:

(a) only those persons identified by name, by function or by office in the accompanying document drawn up when the confidential information was deposited shall be authorised to consult that information;

(b) the application to consult confidential information shall be submitted to the CIU, which shall transfer the document in question to the Secure Reading Room; and

(c) the procedures and conditions governing the consultation of confidential information set out in Article 10 shall apply.

Article 13

Downgrading, declassification and unmarking of confidential information

1. Confidential information may be downgraded, declassified or unmarked only with the prior consent of the originator, and, if necessary, after discussion with other interested parties.

2. Downgrading or declassification shall be confirmed in writing. The originator shall be responsible for informing its addressees of the change, and they in turn shall be responsible for informing any subsequent addressees to whom they have sent or copied the document, of the change. If possible, originators shall specify on classified documents a date, period or event when the contents may be downgraded or declassified. Otherwise, they shall keep the

documents under review every five years, at the latest, in order to ensure that the original classification is necessary.

3. Confidential information held in the secure archives shall be examined in good time, and by no later than the 25th anniversary of its creation, in order to determine whether or not it should be declassified, downgraded or unmarked. The examination and publication of such information shall take place in accordance with the provisions of Council Regulation (EEC, Euratom) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community[4]. Declassification shall be effected by the originator of the classified information or the service currently responsible in accordance with Annex I, Part 1, Section 10.

4. Following declassification, formerly classified information held in the secure archive shall be transferred to the historical archives of the European Parliament for permanent preservation and further treatment under the applicable rules.

5. Following unmarking, formerly 'other confidential information' shall be subject to the European Parliament rules on document management.

Article 14

Breaches of security, loss or compromise of confidential information

1. A breach of confidentiality in general, and of this Decision in particular, shall in the case of Members of the European Parliament entail the application of the relevant provisions concerning penalties set out in the European Parliament's Rules of Procedure.

2. A breach committed by a member of staff of the European Parliament shall lead to the application of the procedures and penalties provided for by, respectively, the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union, laid down in Regulation (EEC, Euratom, ECSC) No 259/68[5] ('the Staff Regulations').

3. The President and/or the Secretary-General, as the case may be, shall organise any necessary investigations in the event of a breach as defined in security notice 6.

4. If the confidential information was communicated to the European Parliament by a Union Institution or by a Member State, the President and/or the Secretary-General, as the case may be, shall inform the Union Institution or Member State concerned of any proven or suspected loss or compromise of classified information, of the results of the investigation and of the measures taken to prevent a recurrence.

Article 15

Adaptation of this Decision and its implementing rules and annual reporting on the application of this Decision

1. The Secretary-General shall propose any necessary adaptation of this Decision and the annexes implementing it and shall forward those proposals to the Bureau for decision.

2. The Secretary-General shall be responsible for the implementation of this Decision by the European Parliament's services and shall issue the handling instructions on matters covered by the ISMS in accordance with the principles laid down by this Decision.

---

[4] OJ L 43, 15.2.1983, p. 1.

[5] OJ L 56, 4.3.1968, p. 1.

3. The Secretary-General shall submit an annual report to the Bureau on the application of this Decision.

Article 16

Transitional and final provisions

1. Non classified information held in the CIU or in any other archive of the European Parliament which is considered as confidential and dated before 1 April 2014 shall be deemed, for the purpose of this Decision, to constitute 'other confidential information'. Its originator may at any time reconsider the level of its confidentiality.

2. By way of derogation from point (a) of Article 5(1) and from Article 8(1) of this Decision, for a period of twelve months from 1 April 2014, information provided by the Council pursuant to the Interinstitutional Agreement which is classified at the level RESTREINT UE/EU RESTRICTED or its equivalent shall be deposited with, registered by and stored in the CIU. Such information may be consulted in accordance with points (a) and (c) of Article 4(2) and with Article 5(4) of the Interinstitutional Agreement.

3. The decision of the Bureau of 6 June 2011 concerning the rules governing the treatment of confidential information by the European Parliament is repealed.

Article 17

Entry into force

This Decision shall enter into force on the day of its publication in the *Official Journal of the European Union*.

ANNEX I

PART 1

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY FOR THE PROTECTION OF CONFIDENTIAL INFORMATION

1.*INTRODUCTION*

These provisions set out the basic principles and minimum standards of security for the protection of confidential information to be respected and/or complied with by the European Parliament in all its places of employment, including by all recipients of, classified information and 'other confidential information' so that security is safeguarded and all persons concerned may be assured that a common standard of protection is established. These provisions are supplemented by the security notices contained in Annex II and by other provisions governing the treatment of confidential information by parliamentary committees and other parliamentary bodies/office-holders.

2.*BASIC PRINCIPLES*

The European Parliament's security policy forms an integral part of its general internal management policy and is thus based on the principles governing that general policy. Those principles include legality, transparency, accountability, subsidiarity and proportionality.

Legality entails the need to remain strictly within the legal framework in the performance of security functions, and to conform to the applicable legal requirements. Furthermore, responsibilities in the field of security must be based on proper legal provisions. The provisions of the Staff Regulations, in particular Article 17 thereof on the obligation of staff to refrain from any unauthorised disclosure of information received in the line of duty and Title VI thereof on disciplinary measures, are fully applicable. Finally, breaches of security within the responsibility of the European Parliament shall be dealt with in a manner consistent with its Rules of Procedure and its policy on disciplinary measures.

Transparency entails the need for clarity regarding all security rules and provisions, for a balance between the different services and the different domains (physical security as compared to the protection of information, etc.), and for a consistent and structured security awareness policy. Moreover, clear written guidelines are necessary for the implementation of security measures.

Accountability means that responsibilities in the field of security must be clearly defined. Moreover, it entails the need regularly to monitor whether those responsibilities have been properly fulfilled.

Subsidiarity means that security must be organised at the lowest possible level and as closely as possible to the European Parliament's Directorates-General and services.

Proportionality means that security activities must be strictly limited to those which are absolutely necessary and that security measures must be proportional to the interests to be protected as well as to the actual or potential threat to those interests, so as to enable those interests to be defended in a manner ensuring the least possible disruption.

3.*FOUNDATIONS OF INFORMATION SECURITY*

The foundations of sound information security are:

(a) proper communication and information systems (CIS). These fall within the responsibility of the European Parliament's Security Authority (as defined in security notice 1);

7.3.3.

(b) within the European Parliament, the Information Assurance Authority (as defined in security notice 1) responsible for working with the Security Authority to provide information and advice on technical threats to CIS and the means of protecting against those threats;

(c) close cooperation between the European Parliament's responsible services and the security services of the other Union institutions;

4.*PRINCIPLES OF INFORMATION SECURITY*

4.1.Objectives

The principle objectives of information security are as follows:

(a) to safeguard confidential information against espionage, compromise or unauthorised disclosure;

(b) to safeguard classified information handled in communications and information systems and networks against threats to its confidentiality, integrity and availability;

(c) to safeguard European Parliament premises housing classified information against sabotage and malicious wilful damage;

(d) in the event of a security failure, to assess the damage caused, limit the consequences, conduct security investigations and adopt any necessary remedial measures.

4.2.Classification

4.2.1. Where confidentiality is concerned, care and experience are needed in the selection of the information and material to be protected as well as in assessing the degree of protection required. It is essential that the degree of protection should correspond to the sensitivity, in terms of security, of the individual item of information or material to be safeguarded. In order to ensure the smooth flow of information, both over-classification and under-classification shall be avoided.

4.2.2. The classification system is the instrument for putting into effect the principles set out in this section. A similar classification system shall be followed in planning and organising ways to counter espionage, sabotage, terrorism and other threats, in order to ensure maximum protection for the most important premises housing classified information and the most sensitive points within those premises.

4.2.3. Responsibility for classifying information lies solely with the originator of the information concerned.

4.2.4. The level of classification may be based solely on the content of the information concerned.

4.2.5. Where several items of information are grouped together, their classification shall be at least as high as the highest classification level assigned to one of its individual items. However, a collection of information may be assigned a higher classification than its constituent parts.

4.2.6. Classifications shall be assigned only when necessary and for as long as necessary.

4.3.Aims of security measures

The security measures shall:

7.3.3.

(a) extend to all persons having access to classified information, media carrying classified information and 'other confidential information', as well as all premises containing such information and important installations;

(b) be designed in such a way as to identify persons whose position (in terms of access, relationships or otherwise) might jeopardise the security of such information and of important installations housing such information, and provide for their exclusion or removal;

(c) prevent unauthorised persons from having access to such information or to installations containing it;

(d) ensure that such information is disseminated solely on the basis of the need-to-know principle, which is fundamental to all aspects of security;

(e) ensure the integrity (by preventing corruption, unauthorised alteration or unauthorised deletion) and the availability (to those needing and authorised to have access thereto) of confidential information, especially where it is stored, processed or transmitted in electromagnetic form.

5.*COMMON MINIMUM STANDARDS*

The European Parliament shall ensure that common minimum standards of security are observed by all recipients of classified information, both inside the institution and under its competence, namely all its services and contractors, so that such information can be passed on in the confidence that it will be handled with equal care. Such minimum standards shall include criteria for the security clearance of officials of the European Parliament and other Parliament employees working for political groups, and procedures for the protection of confidential information.

The European Parliament shall allow third parties access to such information only when such third parties guarantee that it is handled in accordance with provisions that are at least strictly equivalent to these common minimum standards.

Such common minimum standards shall also be applied when, pursuant to a contract or grant, the European Parliament entrusts to industrial or other entities tasks involving confidential information.

6.*SECURITY AS REGARDS OFFICIALS OF THE EUROPEAN PARLIAMENT AND OTHER PARLIAMENT EMPLOYEES WORKING FOR POLITICAL GROUPS*

6.1.Security instructions as regards officials of the European Parliament and other Parliament employees working for political groups

Officials of the European Parliament and other Parliament employees working for political groups in positions where they could have access to classified information shall be given thorough instructions, both on taking up their duties and at regular intervals thereafter, on the need for security and the procedures involved. Such persons shall be required to confirm in writing that they have read and fully understand the applicable security provisions.

6.2.Management responsibilities

It must be part of the duties of managers to know which of their staff are engaged in work on classified information or have access to secure communication or information systems, and to record and report any incidents or apparent vulnerabilities which are likely to affect security.

7.3.3.

6.3.Security status of officials of the European Parliament and other Parliament employees working for political groups

Procedures shall be established to ensure that, when adverse information becomes known concerning an official of the European Parliament or other Parliament employee working for a political group, steps are taken to determine whether that individual's work brings him or her into contact with classified information or whether he or she has access to secure communication or information systems, and that the European Parliament's responsible service is informed. If the competent National Security Authority indicates that such an individual constitutes a security risk, he or she shall be barred or removed from assignments where he or she might endanger security.

7.*PHYSICAL SECURITY*

'Physical security' means the application of physical and technical protective measures to prevent unauthorised access to classified information.

7.1.Need for protection

The degree of physical security measures to be applied to ensure the protection of classified information shall be proportionate to the classification and volume of, and the threat to, the information and material held. All holders of classified information shall follow uniform practices regarding classification of such information and must meet common standards of protection regarding the custody, transmission and disposal of information and material requiring protection.

7.2.Checking

Before leaving areas containing classified information unattended, persons having custody thereof shall ensure that it is securely stored and that all security devices have been activated (locks, alarms, etc.). Further independent checks shall be carried out after working hours.

7.3.Security of buildings

Buildings housing classified information or secure communication and information systems shall be protected against unauthorised access.

The nature of the protection afforded to classified information, e.g. barring of windows, locks for doors, guards at entrances, automated access control systems, security checks and patrols, alarm systems, intrusion detection systems and guard dogs, shall depend on:

(a) the classification, volume and location within the building of the information and material to be protected;

(b) the quality of the security containers for the information and material concerned; and

(c) the physical nature and location of the building.

The nature of the protection afforded to communication and information systems shall depend on an assessment of the value of the assets at stake and of the potential damage if security were to be compromised, on the physical nature and location of the building in which the system is housed, and on the location of that system within the building.

7.4.Contingency plans

Detailed plans shall be in place in advance to ensure the protection of classified information in the event of an emergency.

7.3.3.

8.*SECURITY DESIGNATORS, MARKINGS, AFFIXING AND CLASSIFICATION MANAGEMENT*

8.1.Security designators

No classifications other than those defined in point (d) of Article 2 of this Decision are permitted.

An agreed security designator may be used to set limits to the validity of a classification (for classified information signifying automatic downgrading or declassification).

Security designators shall only be used in combination with a classification.

Security designators are further regulated in security notice 2 and defined in the handling instructions.

8.2.Markings

A marking is used to specify predefined specific instructions about the handling of confidential information. Markings may also indicate the field covered by a given document, a particular distribution on a need-to-know basis, or (for non-classified information) to signify the end of an embargo.

A marking is not a classification and shall not be used in lieu of one.

Markings are further regulated in security notice 2 and defined in the handling instructions.

8.3.Affixing of classifications and of security designators

Affixing of classifications and security designators and markings shall be done in accordance with security notice 2, section E, and the handling instructions.

8.4.Classification management

8.4.1*General*

Information shall be classified only when necessary. The classification shall be clearly and correctly indicated, and shall be maintained only as long as the information requires protection.

The responsibility for classifying information and for any subsequent downgrading or declassification rests solely with the originator.

Officials of the European Parliament shall classify, downgrade or declassify information on instructions from, or pursuant to a delegation from, the Secretary-General.

The detailed procedures for the treatment of classified documents shall be so framed as to ensure that they are afforded protection appropriate to the information which they contain.

The number of persons authorised to originate information classified at the level TRÈS SECRET UE/EU TOP SECRET' shall be kept to a minimum, and their names shall be recorded on a list drawn up by the CIU.

8.4.2*Application of classification*

The classification of a document shall be determined by the level of sensitivity of its contents in accordance with the definitions contained in point (d) of Article 2. It is important that classifications be assigned correctly and used sparingly.

The classification of a letter or note containing enclosures shall be at least as high as the highest classification assigned to one of its enclosures. The originator shall indicate clearly the level at which the letter or note should be classified when detached from its enclosures.

7.3.3.

The originator of a document that is to be given a classification shall follow the rules set out above and shall avoid over-classification or under-classification.

Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classifications and shall be classified accordingly. The classification of the document as a whole shall be that of its most highly classified part.

9.*INSPECTIONS*

Periodic internal inspections of security arrangements for the protection of classified information shall be carried out by the European Parliament's Directorate for Security and Risk Assessment, which may request assistance from the Security Authorities of the Council or of the Commission.

The Security Authorities and competent services of the Union Institutions may carry out, as part of an agreed process initiated by either side, peer evaluations of the security arrangements for the protection of classified information exchanged under the relevant interinstitutional agreements.

10.*DECLASSIFICATION AND UNMARKING PROCEDURES*

10.1. The CIU shall examine confidential information contained in its Register and seek the consent of the originator to the declassification or unmarking of a document by no later than the 25th anniversary of its creation. Documents not declassified or unmarked at the first examination shall be re-examined periodically and at least every five years. In addition to being applied to documents actually located in the secure archives in the Secure Area and duly classified, the unmarking process may also cover other confidential information held either in the parliamentary body/officeor in the service in charge of the Parliament's historical archives.

10.2 The decision with regard to the declassification or unmarking of a document shall, as a general rule, be taken solely by the originator or, exceptionally, in cooperation with the parliamentary body/office-holder of such information, before the information which it contains is transferred to the service in charge of the Parliament's historical archives. Classified information may only be declassified or unmarked with the prior written consent of the originator. In the case of ‘other confidential information’, the secretariat of the parliamentary body/office-holder of such information shall, in cooperation with the originator, decide whether the document can be unmarked.

10.3. On behalf of the originator, the CIU shall be responsible for informing the addressees of the document of the change to the classification or marking, and they in turn shall be responsible for informing any subsequent addressees to whom they have sent or copied the document.

10.4. Declassification shall not affect any security designators or markings which may appear on the document.

10.5. In the case of declassification, the original classification at the top and bottom of every page shall be crossed out. The first (cover) page of the document shall be stamped and completed with the reference of the CIU. In the case of unmarking, the original marking at the top of every page shall be crossed out.

10.6. The text of the declassified or unmarked document shall be attached to the electronic fiche or equivalent system where it has been registered.

10.7. In the case of documents covered by the exception relating to privacy and the integrity of the individual or commercial interests of a natural or legal person, and in the case of sensitive documents, Article 2 of Regulation (EEC, Euratom) No 354/83 shall apply.

7.3.3.

10.8. In addition to the provisions of points 10.1 to 10.7, the following rules shall apply:

(a) as regards third-party documents, the CIU shall consult the third party concerned before proceeding to carry out the declassification or unmarking;

(b) as regards the exception relating to privacy and the integrity of the individual, the declassification or unmarking procedure shall take into account, in particular, the agreement of the person concerned or, as the case may be, the impossibility of identifying the person concerned;

(c) as regards the exception relating to commercial interests of a natural or legal person, the person concerned may be notified via publication in the *Official Journal of the European Union* and given four weeks from the date of that publication in which to submit remarks.

PART 2

SECURITY CLEARANCE PROCEDURE

11.*SECURITY CLEARANCE PROCEDURE FOR MEMBERS OF THE EUROPEAN PARLIAMENT*

11.1. In order to have access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent, Members of the European Parliament shall have been authorised either in accordance with the procedure referred to in points 11.3 and 11.4 of this Annex or on the basis of a solemn declaration of non-disclosure pursuant to Article 3(4) of this Decision.

11.2 In order to have access to information classified at the level SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent, Members of the European Parliament shall have been authorised in accordance with the procedure referred to in points 11.3 and 11.14.

11.3. Authorisation shall be granted only to Members of the European Parliament who have undergone security screening by the competent national authorities of the Member States in accordance with the procedure referred to in points 11.9 to 11.14. The President shall be responsible for granting the authorisation for Members.

11.4 The President may grant written authorisation after obtaining the opinion of the competent national authorities of the Member States on the basis of security screening carried out in accordance with points 11.8 to 11.13.

11.5. The European Parliament's Directorate for Security and Risk Assessment shall maintain an up-to-date list of all Members of the European Parliament who have been granted authorisation, including provisional authorisation within the meaning of point 11.15.

11.6. Authorisation shall be valid for a period of five years or for the duration of the tasks in respect of which it was granted, whichever is the shorter. It may be renewed in accordance with the procedure laid down in point 11.4.

11.7. Authorisation shall be withdrawn by the President where he/she considers that there are justified grounds for such withdrawal. Any decision to withdraw authorisation shall be notified to the Member of the European Parliament concerned, who may ask to be heard by the President before the withdrawal takes effect, and to the competent national authority.

11.8. Security screening shall be carried out with the assistance of the Member of the European Parliament concerned and at the request of the President. The competent national

authority for screening shall be that of the Member State of which the Member concerned is a national.

11.9. As part of the screening procedure, the Member of the European Parliament concerned shall be required to complete a personal information form.

11.10. The President shall specify in his/her request to the competent national authority the level of classified information to be made available to the Member of the European Parliament concerned, so that it may carry out the screening process.

11.11 The entire security-screening process carried out by the competent national authority, together with the results obtained, shall be in accordance with the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.

11.12. Where the competent national authority gives a positive opinion, the President may grant the Member of the European Parliament concerned authorisation.

11.13. A negative opinion by the competent national authority shall be notified to the Member of the European Parliament concerned, who may ask to be heard by the President. Should he/she consider it necessary, the President may ask the competent national authority for further clarification. If the negative opinion is confirmed, authorisation shall not be granted.

11.14. All Members of the European Parliament who are granted authorisation within the meaning of point 11.3 shall, at the time when the authorisation is granted and at regular intervals thereafter, receive any necessary guidelines concerning the protection of classified information and the means of ensuring such protection. Such Members shall sign a declaration acknowledging receipt of those guidelines.

11.15. In exceptional circumstances, the President may, after notifying the competent national authority and provided that no reaction is received from that authority within one month, grant provisional authorisation to a Member of the European Parliament for a period not exceeding six months, pending the outcome of the screening referred to in point 11.11. Provisional authorisations thus granted shall not give access to information classified at the level TRÈS SECRET UE/EU TOP SECRET or its equivalent.

12. *SECURITY CLEARANCE PROCEDURE FOR OFFICIALS OF THE EUROPEAN PARLIAMENT AND OTHER PARLIAMENT EMPLOYEES WORKING FOR POLITICAL GROUPS*

12.1. Only officials of the European Parliament and other Parliament employees working for political groups who, by reason of their duties and the requirements of the service, need to have knowledge of, or to use, classified information may have access thereto.

12.2. In order to have access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, or TRÈS SECRET UE/EU TOP SECRET, or its equivalent, the officials of the European Parliament and other Parliament employees working for political groups concerned shall have been authorised in accordance with the procedure laid down in points 12.3 and 12.4.

12.3. Authorisation shall be granted only to the persons referred to in point 12.1 who have undergone security screening by the competent national authorities of the Member States in accordance with the procedure referred to in points 12.9 to 12.14. The Secretary-General shall be responsible for granting the authorisation for officials of the European Parliament and other Parliament employees working for political groups.

12.4 The Secretary-General may grant written authorisation after obtaining the opinion of the competent national authorities of the Member States on the basis of security screening carried out in accordance with points 12.8 to 12.13.

7.3.3.

12.5. The European Parliament's Directorate for Security and Risk Assessment shall maintain an up-to-date list of all posts requiring a security clearance, as provided by the relevant European Parliament services, and of all persons who have been granted authorisation, including provisional authorisation within the meaning of point 12.15.

12.6. Authorisation shall be valid for a period of five years or for the duration of the tasks in respect of which it was granted, whichever is the shorter. It may be renewed in accordance with the procedure referred to in point 12.4.

12.7. Authorisation shall be withdrawn by the Secretary-General where he/she considers that there are justifiable grounds for such withdrawal. Any decision to withdraw authorisation shall be notified to the official of the European Parliament or other Parliament employee working for a political group concerned, who may ask to be heard by the Secretary-General before the withdrawal takes effect, and to the competent national authority.

12.8. Security screening shall be carried out with the assistance of the official of the European Parliament or other Parliament employee working for political groups concerned and at the request of the Secretary-General. The competent national authority for screening shall be that of the Member State of which the person concerned is a national. Where permissible under national laws and regulations, the competent national authorities may conduct investigations in respect of non-nationals who require access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET.

12.9. As part of the screening procedure, the official of the European Parliament or other Parliament employee working for a political group concerned shall be required to complete a personal information form.

12.10. The Secretary-General shall specify in his/her request to the competent national authority the level of classified information to be made available to the official of the European Parliament or other Parliament employee working for political groups concerned, so that it may carry out the screening process and give its opinion as to the level of authorisation appropriate to be granted to that person.

12.11. The entire security-screening process carried out by the competent national authority, together with the results obtained, shall be in accordance with the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.

12.12. Where the competent national authority gives a positive opinion, the Secretary-General may grant the official of the European Parliament or other Parliament employee working for political groups concerned authorisation.

12.13. A negative opinion by the competent national authority shall be notified to the official of the European Parliament or other Parliament employee working for a political group concerned, who may ask to be heard by the Secretary-General. Should he/she consider it necessary, the Secretary-General may ask the competent national authority for further clarification. If the negative opinion is confirmed, authorisation shall not be granted.

12.14. All officials of the European Parliament and other Parliament employees working for political groups who are granted authorisation within the meaning of points 12.4 and 12.5 shall, at the time when the authorisation is granted and at regular intervals thereafter, receive any necessary instructions concerning the protection of classified information and the means of ensuring such protection. Such officials and employees shall sign a declaration acknowledging receipt of those instructions and give an undertaking to obey them.

12.15. In exceptional circumstances, the Secretary-General may, after notifying the competent national authority and provided that no reaction is received from that authority within one

7.3.3.

month, grant provisional authorisation to an official of the European Parliament or other Parliament employee working for a political group for a period not exceeding six months, pending the outcome of the screening referred to in point 12.11. Provisional authorisations thus granted shall not give access to information classified at the level TRÈS SECRET UE/EU TOP SECRET or its equivalent.

ANNEX II

INTRODUCTION

These provisions lay down the security notices governing and ensuring the secure treatment and management of confidential information by the European Parliament. Those security notices, together with the handling instructions, constitute the European Parliament's information security management system (ISMS) referred to in Article 3(2) of this Decision:

SECURITY NOTICE 1

The organisation of security in the European Parliament for the protection of confidential information

SECURITY NOTICE 2

Management of confidential information

SECURITY NOTICE 3

The processing of confidential information by means of automated communication information systems (CIS)

SECURITY NOTICE 4

Physical security

SECURITY NOTICE 5

Industrial security

SECURITY NOTICE 6

Breaches of security, loss or compromise of confidential information

SECURITY NOTICE 1

THE ORGANISATION OF SECURITY IN THE EUROPEAN PARLIAMENT FOR THE PROTECTION OF CONFIDENTIAL INFORMATION

1. The Secretary-General shall be responsible for the overall and consistent implementation of this Decision.

The Secretary-General shall take all necessary measures to ensure that, for the purposes of handling or storing confidential information, this Decision is applied in Parliament's premises, by Members of the European Parliament, by officials of the European Parliament, by other Parliament employees working for political groups and by contractors.

2. The Secretary-General is the Security Authority (SA). In this capacity, the Secretary-General shall be responsible for:

2.1. coordinating all matters of security relating to Parliament's activities in relation to the protection of confidential information;

2.2. approving the installation of a Secure Area, Secure Reading Rooms and secure equipment;

7.3.3.

2.3. implementing decisions authorising, pursuant to Article 6 of this Decision, the transmission of classified information by Parliament to third parties;

2.4. investigating or ordering an investigation into any leakage of confidential information which prima facie has occurred within Parliament, in liaison with the President of the European Parliament, where a Member of the European Parliament is concerned;

2.5. maintaining close contact with the security authorities of other Union Institutions and with National Security Authorities in the Member States with a view to ensuring optimal coordination of security policy related to classified information;

2.6. keeping Parliament's security policy and procedures constantly under review and issuing appropriate recommendations resulting therefrom;

2.7. reporting to the National Security Authority (NSA) which has carried out the security screening procedure, in accordance with Annex I, Part 2, point 11.3, in cases involving any adverse information which may affect that authority.

3. Where a Member of the European Parliament is concerned, the Secretary-General shall discharge his/her responsibilities in close liaison with the President of the European Parliament.

4. In fulfilling his/her responsibilities under paragraphs 2 and 3, the Secretary-General shall be assisted by the Deputy Secretary-General, the Directorate for Security and Risk Assessment, the Directorate for Information Technologies (DIT) and the Classified Information Unit (CIU).

4.1. The Directorate for Security and Risk Assessment shall be responsible for personal protection measures and, in particular, for the security clearance procedure, as laid down in Annex I, Part 2. The Directorate for Security and Risk Assessment shall also:

(a) be the point of contact for the security authorities of the other Union Institutions and for the NSAs, in matters relating to security clearance procedures for Members of the European Parliament, officials of the European Parliament and other Parliament employees working for political groups;

(b) provide the necessary general security briefing on the obligation to protect classified information and on the consequences of any failure to do so;

(c) monitor the operation of the Secure Area and the Secure Reading Rooms within Parliament's premises, in cooperation, where appropriate, with the security services of the other Union Institutions and the NSAs;

(d) audit, in cooperation with the security authorities of the other Union Institutions and the NSAs, the procedures for the management and storage of classified information, the Secure Area and the Secure Reading Rooms within Parliament's premises where classified information is handled;

(e) propose the appropriate handling instructions to the Secretary-General.

4.2. The DIT shall be responsible for handling of confidential information by secure IT systems at the European Parliament.

4.3. The CIU shall be responsible for:

(a) identifying the security needs for the effective protection of confidential information, in close cooperation with the Directorate for Security and Risk Assessment and DITand with the Security Authorities of the other Union Institutions;

7.3.3.

(b) identifying all aspects of the management and storage of confidential information within Parliament, as laid down in the handling instructions;

(c) the operation of the Secure Area;

(d) the management or consultation of confidential information in the Secure Area or in the CIU's Secure Reading Room, in accordance with paragraghs (2) and (3) of Article 7 of this Decision;

(e) the management of the CIU Register;

(f) reporting to the SA any proven or suspected breach of security, loss or compromise relating to confidential information deposited at the CIU and held in the Secure Area or in the CIU Secure Reading Room.

5. Furthermore, the Secretary-General, as SA, shall appoint the following authorities:

(a) a Security Accreditation Authority (SAA);

(b) an Information Assurance Operational Authority (IAOA);

(c) a Crypto Distribution Authority (CDA);

(d) a TEMPEST Authority (TA);

(e) an Information Assurance Authority (IAA).

The exercise of those functions does not require single organisational entities. They shall have separate mandates. However, those functions, and their accompanying responsibilities, may be combined or integrated in the same organisational entity or split into different organisational entities, provided that conflicts of interest and duplication of tasks are avoided.

6. The SAA shall advise on all security matters related to the accreditation of each information technology system and network within Parliament by:

6.1. ensuring that the CIS comply with the relevant security policies and security guidelines, providing a statement of approval for the handling by the CIS of classified information to a defined level of classification in its operational environment and stating the terms and conditions of the accreditation and the criteria under which re-approval is required;

6.2. setting up a security accreditation process, in accordance with the relevant policies, clearly stating the approval conditions for the CIS under its authority;

6.3. drawing up a security accreditation strategy which sets out the degree of detail for the accreditation process commensurate with the level of assurance required;

6.4. examining and approving security-related documentation, including risk management and residual risk statements, security implementation verification documentation and security operating procedures, and ensuring that it complies with Parliament's security rules and policies;

6.5. verifying the implementation of security measures in relation to the CIS by carrying out or sponsoring security assessments, inspections or reviews;

6.6. identifying security requirements (e.g. personnel clearance levels) for sensitive positions in relation to the CIS;

6.7. approving, or where relevant, participating in, the joint approval of the interconnection of a given CIS to other CIS;

6.8. approving the security standards of technical equipment envisaged for the secure handling and protection of classified information;

7.3.3.

6.9. ensuring that cryptographic products used within Parliament are included in the list of EU approved products; and

6.10. consulting the system provider, the security actors and representatives of the users with respect to security risk management, in particular the residual risk, and the terms and conditions of the approval statement.

7. The IAOA shall be responsible for:

7.1. developing security documentation in line with security policies and security guidelines, in particular including the residual risk statement, the security operating procedures and the crypto plan within the CIS accreditation process;

7.2. participating in the selection and testing of the system-specific technical security measures, devices and software, in order to supervise their implementation and to ensure that they are securely installed, configured and maintained in accordance with the relevant security documentation;

7.3. monitoring the implementation and application of the security operating procedures and, where appropriate, delegating operational security responsibilities to the system owner, namely the CIU;

7.4. managing and handling cryptographic products, ensuring the custody of crypto items and controlled items and, if so required, ensuring the generation of cryptographic variables;

7.5. conducting security analysis reviews and tests, in particular for the purposes of producing the relevant risk reports, as required by the SAA;

7.6. providing CIS-specific information assurance training;

7.7. implementing and operating CIS-specific security measures.

8. The CDA shall be responsible for:

8.1. managing and accounting for EU crypto material;

8.2. ensuring, in close cooperation with the SAA, that appropriate procedures are enforced and that plans are in place for accounting, secure handling, storage and distribution of all EU crypto material; and

8.3. ensuring the transfer of EU crypto material to or from individuals or services using it.

9. The TA shall be responsible for ensuring compliance by the CIS with TEMPEST policies and handling instructions. It shall approve TEMPEST countermeasures for installations and products to protect classified information to a defined level of classification in its operational environment.

10. The IAA shall be responsible for all aspects of the management and handling of confidential information within Parliament and, in particular, for:

10.1 developing information assurance security and its security guidelines, and monitoring their effectiveness and pertinence;

10.2. safeguarding and administering technical information related to cryptographic products;

10.3. ensuring that information assurance measures selected for protecting classified information comply with the relevant policies governing their eligibility and selection;

7.3.3.

10.4. ensuring that cryptographic products are selected in compliance with policies governing their eligibility and selection;

10.5. consulting with the system provider, the security actors and representatives of users with regard to information assurance security;

SECURITY NOTICE 2

MANAGEMENT OF CONFIDENTIAL INFORMATION

A.*INTRODUCTION*

1. This security notice sets out the provisions for the management by Parliament of confidential information.

2. When creating confidential information, the originator shall assess the level of confidentiality and take a decision based on the principles set out in this security notice as to the classification or marking of that information.

B.*EUCI CLASSIFICATION*

3. The decision to classify a document shall be made before its creation. To that end, classifying information as EUCI involves a prior assessment of its level of confidentiality and a decision by the originator that unauthorised disclosure of such information would cause some degree of prejudice to the interests of the European Union or of one or more of its Member States or individuals.

4. Once the decision to classify the information is taken, a second prior assessment shall follow in order to determine the appropriate classification level. The classification of a document shall be determined by the level of sensitivity of its contents.

5. Responsibility for classifying information shall lie solely with the originator. Parliament officials shall classify information on instructions from, or pursuant to a delegation by, the Secretary-General.

6. Classification shall be correctly and sparingly used. The originator of a document that is to be given a classification shall curb any tendency to over-classify or under-classify.

7. The classification level assigned to the information shall determine the level of protection afforded to it in the areas of personnel security, physical security, procedural security and information assurance.

8. Information which warrants classification shall be marked and handled as such, regardless of its physical form. Its classification shall be clearly communicated to its recipients, either by a security classification marking (if it is delivered in written form, be it on paper or within a CIS) or by an announcement (if it is delivered in oral form, such as in the course of a conversation or a meeting held in camera). Classified material shall be physically marked so as to enable its security classification to be easily identified.

9. EUCI in electronic form may only be created within an accredited CIS. The classified information itself, as well as the file name and storage device (if external, such as a CD-ROM or USB stick), shall bear the relevant security classification marking.

10. Information shall be classified as soon as it takes form. For example, personal notes, drafts or e-mail messages containing information which warrants classification are to be marked as EUCI from the outset and shall be produced and handled in accordance with this Decision and its handling instructions in physical and technical terms. Such information may then evolve into an official document which will in turn be appropriately marked and handled.

7.3.3.

During the drafting process, an official document may need to be re-evaluated and assigned a higher or lower classification level as it evolves.

11. The originator may decide to assign a standard classification level to categories of information which he/she creates on a regular basis. However, the originator shall ensure that, in so doing, he/she does not systematically over-classify or under-classify individual pieces of information.

12. EUCI shall always bear a security classification marking corresponding to its security classification level.

B.1.Levels of classification

13. EUCI shall be classified at one of the following levels:

– ‘TRÈS SECRET UE/EU TOP SECRET’, as defined in point (d) of Article 2 of this Decision, where its compromise would be likely to:

(a) threaten directly the internal stability of the Union or of one or more of its Member States or third States or international organisations;

(b) cause exceptionally grave damage to relations with third States or international organisations;

(c) lead directly to widespread loss of life;

(d) cause exceptionally grave damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the continuing effectiveness of extremely valuable security or intelligence operations; or

(e) cause severe long-term damage to the Union's or Member States' economy;

– ‘SECRET UE/EU SECRET’, as defined in point (d) of Article 2 of this Decision, where its compromise would be likely to:

(a) raise international tensions to a significant degree;

(b) seriously damage relations with third States and international organisations;

(c) threaten life directly or seriously prejudice public order or individual security or liberty;

(d) damage major commercial or policy negotiations, causing significant operational problems for the Union or Member States;

(e) cause serious damage to the operational security of Member States, or to the effectiveness of highly valuable security or intelligence operations;

(f) cause substantial material damage to Union or Member State financial, monetary, economic and commercial interests;

(g) substantially undermine the financial viability of major organisations or operators; or

(h) seriously impede the development or operation of Union policies with major economic, trade or financial consequences;

– ‘CONFIDENTIEL UE/EU CONFIDENTIAL’, as defined in point (d) of Article 2 of this Decision, where its compromise would be likely to:

(a) significantly damage diplomatic relations, e.g. where it would lead to a formal protest or other sanctions;

7.3.3.

(b) put individual security or liberty at risk;

(c) put the outcome of commercial or policy negotiations at serious risk; cause operational problems for the Union or Member States;

(d) cause damage to the operational security of Member States, or to the effectiveness of security or intelligence operations;

(e) substantially undermine the financial viability of major organisations or operators;

(f) impede the investigation or facilitate the commission of crime or terrorist activities;

(g) work substantially against Union or Member State financial, monetary, economic and commercial interests; or

(h) seriously impede the development or operation of Union policies with major economic, trade or financial consequences;

– 'RESTREINT UE/EU RESTRICTED', as defined in point (d) of Article 2 of this Decision, where its compromise would be likely to:

(a) be disadvantageous to the general interests of the Union;

(b) adversely affect diplomatic relations;

(c) cause substantial distress to individuals or companies;

(d) be disadvantageous to the Union or Member States in commercial or policy negotiations;

(e) make it more difficult to maintain effective security within the Union or Member States;

(f) impede the effective development or operation of Union policies;

(g) undermine the proper management of the Union and its operations;

(h) breach undertakings given by Parliament to maintain the classified status of information provided by third parties;

(i) breach statutory restrictions on disclosure of information;

(j) cause financial loss or facilitate improper gain or advantage for individuals or companies; or

(k) prejudice the investigation or facilitate the commission of crime.

B.2.Classification of compilations, cover pages and excerpts

14. The classification of a letter or note containing enclosures shall be as high as the highest classification level assigned to one of its enclosures. The originator shall indicate clearly the level at which the letter or note should be classified when detached from its enclosures. Where the cover note/letter does not need to be classified, it shall include the following final wording: 'When detached from its enclosures, this note/letter is unclassified.'.

15. Documents or files containing components with different classification levels are whenever possible to be structured in such a way that components with a different classification level may be easily identified and detached if necessary. The overall classification level of a document or file shall be at least as high as that of its most highly classified component.

7.3.3.

16. Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classification levels and shall be classified accordingly. Standard abbreviations may be used within documents containing EUCI to indicate the classification level of sections or blocks of text of less than a single page.

17. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification level than its component parts.

C.*OTHER CONFIDENTIAL INFORMATION*

18. 'Other confidential information' shall be marked in accordance with point E of this security notice and the handling instructions.

D.*CREATION OF CONFIDENTIAL INFORMATION*

19. Only persons duly empowered by this Decision or authorised by the SA may create confidential information.

20. Confidential information shall not be added to internet or intranet document management systems.

D.1.Creation of EUCI

21. In order to create EUCI classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, the individual concerned shall be empowered by this Decision or shall first be in possession of an authorisation granted pursuant to Article 4(1) of this Decision.

22. EUCI classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET shall be created only within the Secure Area.

23. The following rules shall apply to the creation of EUCI:

(a) each page shall be marked clearly with the applicable classification level;

(b) each page shall be numbered and shall state the total number of pages;

(c) the document shall bear a reference number on the first page and an indication of its subject-matter, which shall not itself constitute classified information, unless it is affixed as such;

(d) the document shall bear a date on the first page;

(e) the first page of any document classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET shall contain a list of all annexes and enclosures;

(f) documents classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET shall bear a copy number on every page, if they are to be distributed in several copies. Each copy shall also bear on the first page the total number of copies and of pages, and

(g) if the document makes reference to other documents containing classified information received from other Union Institutions, or if it contains classified information emanating from those documents, it shall bear the same classification level as those documents and may not, without the prior written consent of its originator, be distributed to any persons other than those named in the distribution list in respect of the original document or documents containing classified information.

7.3.3.

24. The originator shall retain control of EUCI which he/she has created. His/her prior written consent shall be sought before that EUCI is:

(a) downgraded or declassified;

(b) used for purposes other than those established by the originator;

(c) disclosed to any third State or international organisation;

(d) disclosed to any person, institution, country or international organisation other than the addressees originally authorised by the originator to consult the information in question;

(e) disclosed to a contractor or prospective contractor located in a third State;

(f) copied or translated, if the information is classified at the level TRES SECRET UE/EU TOP SECRET;

(g) destroyed.

D.2.Creation of other confidential information

25. The Secretary-General, acting as SA, may decide whether or not to authorise the creation of 'other confidential information' by a given function, service and/or individual.

26. 'other confidential information' shall bear one of the markings defined in the handling instructions.

27. The following rules shall apply to the creation of 'other confidential information':

(a) its marking shall be indicated at the top of the first page of the document;

(b) each page shall be numbered within the total number of pages;

(c) the document shall bear a reference number on the first page and an indication of its subject-matter;

(d) the document shall bear a date on the first page and;

(e) the last page of the document shall contain a list of all annexes and enclosures.

28. Creation of 'other confidential information' is subject to specific rules and procedures laid down in the handling instructions.

E.*SECURITY DESIGNATORS AND MARKINGS*

29. Security designators and markings on documents are intended to control the flow of information and to restrict access to confidential information on the basis of the 'need to know' principle.

30. When security designators and/or markings are being used or affixed, care shall be taken to avoid confusion with security classifications for EUCI: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.

31. Specific rules concerning the use of security designators and markings, along with the list of approved European Parliament security markings, shall be laid down in the handling instructions.

E.1.Security designators

32. Security designators may only be used in conjunction with a security classification and shall not be applied separately to documents. A security designator may be applied to EUCI in order to:

7.3.3.

(a) set limits to the validity of a classification (for classified information signifying automatic downgrading or declassification);

(b) limit the distribution of the EUCI in question;

(c) establish special handling arrangements in addition to those corresponding to the security classification level.

33. The extra controls applicable to the handling and storage of documents containing EUCI impose additional burdens on all involved. In order to minimise the work required in this connection, it is good practice, when creating such a document, to establish a time limit or event after which the classification is to automatically expire and the information contained in the document is to be downgraded or declassified.

34. Where a document deals with a specific area of work and its distribution needs to be limited and/or it is to be subject to special handling arrangements, a statement to that effect may be added to its classification to help to identify its target audience.

E.2.Markings

35. Markings do not constitute a security classification. They are intended to serve only to provide concrete instructions about the handling of a document, and shall not be used to describe the contents of such document.

36. Markings may be applied separately to documents or used in conjunction with a security classification.

37. As a general rule, markings shall be applied to information which is covered by the professional secrecy referred to in Article 339 TFEU and Article 17 of the Staff Regulations, or which has to be protected for legal reasons by Parliament but does not need to be, or cannot be, classified.

E.3.Use of markings in the CIS

38. The rules on the use of the markings are also applicable within the accredited CIS.

39. The SAA shall establish specific rules on the use of markings in the accredited CIS.

F.*RECEPTION OF INFORMATION*

40. Only the CIU shall be entitled within Parliament to receive information classified as CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent from third parties.

41. As to information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and ‘other confidential information’, both the CIU or the competent parliamentary body/office-holder may be responsible for receiving it from third parties, and for applying the principles set out in this security notice.

G.*REGISTRATION*

42. Registration means the application of procedures for recording the life-cycle of confidential information, including its dissemination, consultation and destruction.

43. For the purposes of this security notice, ‘logbook’ means a register which records in particular the dates and times when confidential information:

(a) enters or exits the respective secretariat of the parliamentary body/office-holder or, as the case may be, the CIU;

(b) is accessed by or transmitted to a security-cleared person; and

(c) is destroyed.

7.3.3.

44. The originator of classified information shall be responsible for marking the initial declaration upon the creation of a document containing such information. That declaration shall be communicated to the CIU when the document is created.

45. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent may only be registered by the CIU for security purposes. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' received from third parties shall be registered by the service responsible for the official reception of the document, being either the CIU or the secretariat of the parliamentary body/office-holder, for administrative purposes. 'Other confidential information' produced within Parliament shall be registered by the originator, for administrative purposes.

46. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall be registered especially when:

(a) it is produced;

(b) it arrives at or leaves the CIU; and

(c) it arrives at or leaves the CIS.

47. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent shall be registered especially when:

(a) it is produced;

(b) it arrives at or leaves the respective secretariat of the parliamentary body/office-holder or the CIU; and

(c) it arrives at or leaves the CIS.

48. Registration of confidential information may be carried out on paper or in electronic logbooks/CIS.

49. For information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information', at least the following shall be recorded:

(a) the date and time when it enters or leaves the respective secretariat of the parliamentary body/office-holder or the CIU, as the case may be;

(b) the document title, the classification level or marking, the expiry date of the classification/marking and any reference number assigned to the document.

50. For information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent, at least the following shall be recorded:

(a) the date and time when it enters or leaves the CIU;

(b) the document title, classification level or marking, any reference number assigned to the document and the expiry date of the classification/marking;

(c) details of the originator;

(d) a record of the identity of any person who is given access to the document, and of the date when it was accessed by that person;

(e) a record of any copies or translations made of the document;

(f) the date and time when any copies or translations of the document leave or return to the CIU, and details of where they have been sent and who has returned them;

7.3.3.

(g) the date and time when the document is destroyed, and by whom, in accordance with Parliament's security rules on destruction; and

(h) the declassification or downgrading of the document.

51. Logbooks shall be classified or marked as appropriate. Logbooks for information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent shall be registered at the same level.

52. Classified information may be registered:

(a) in a single logbook; or

(b) in separate logbooks according to its classification level, its status as incoming or outgoing information and its origin or destination.

53. In the case of electronic handling within the CIS, registration procedures may be carried out by those means within the CIS itself which meet requirements equivalent to those specified above. Whenever EUCI leaves the perimeter of the CIS, the registration procedure described above shall apply.

54. The CIU shall keep a record of all classified information released by Parliament to third parties and of classified information received by Parliament from third parties.

55. Once registration of information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent is complete, the CIU shall check whether the addressee has a valid security authorisation. Where this is the case, the addressee shall be notified by the CIU. The consultation of classified information may only take place once the document containing it has been registered.

H.*DISTRIBUTION*

56. The originator shall establish the initial distribution list for the EUCI which he/she has created.

57. Information classified at the level RESTREINT UE/EU RESTRICTED and 'other confidential information' produced by Parliament shall be distributed within Parliament by the originator, in accordance with the relevant handling instructions and on the basis of the 'need-to-know' principle. For information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET created by Parliament within the Secure Area, the distribution list (and any further instructions concerning distribution) shall be provided to the CIU, which shall be responsible for its management.

58. EUCI produced by Parliament may be distributed to third parties only by the CIU, on the basis of the 'need to know' principle.

59. Confidential information received either by the CIU or by any parliamentary body/office-holder who submitted the request therefor shall be distributed in accordance with the instructions received from the originator.

I.*HANDLING, STORAGE AND CONSULTATION*

60. Handling, storage and consultation of confidential information shall be carried out in accordance with security notice 4 and the handling instructions.

J.*COPYING/TRANSLATING/INTERPRETING CLASSIFIED INFORMATION*

61. Documents containing information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent shall not be copied or translated without the prior written consent

of the originator. Documents containing information classified at the level SECRET UE/EU SECRET or its equivalent or at the level CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent may be copied or translated on instruction from the holder, provided the originator has not prohibited this.

62. Each copy of a document containing information classified at the level TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET or CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent shall be registered for security purposes.

63. The security measures applicable to the original document containing classified information shall apply to copies and translations thereof.

64. Documents received from the Council should be received in all official languages.

65. Copies and/or translations of documents containing classified information may be requested by the originator or copy holder. Copies of documents containing information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent may only be produced in the Secure Area and on copiers which are part of an accredited CIS. Copies of documents containing information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' shall be made using an accredited reproduction device within Parliament's premises.

66. All copies and translations of any document or parts of copies of documents containing confidential information shall be appropriately marked, numbered and registered.

67. No more copies shall be made than are strictly necessary. All copies shall be destroyed in accordance with the handling instructions at the end of the consultation period.

68. Only interpreters and translators who are Parliament officials shall ge given access to classified information.

69. Interpreters and translators with access to documents containing information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall have the appropriate security clearance.

70. When working on documents containing information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET,or its equivalent, interpreters and translators shall work in the Secure Area.

K.*DOWNGRADING, DECLASSIFYING AND UNMARKING OF CONFIDENTIAL INFORMATION*

K.1.General principles

71. Confidential information shall be declassified, downgraded or unmarked when protection is no longer necessary or is no longer needed at the original level.

72. Decisions to downgrade, declassify or unmark information contained in documents produced within Parliament may also have to be made on an ad hoc basis, for example in response to a request for access from the public or from another Union Institution, or at the initiative of the CIU or parliamentary body/office-holder.

73. At the time of its creation, the originator of EUCI shall indicate, where possible, whether the EUCI in question can be downgraded or declassified on a given date or following a specific event. When it is not practicable to give such an indication, the originator, the CIU or the parliamentary body/office-holder holding the information shall review the classification

level of EUCI at least once every five years. In all instances, EUCI may be downgraded or declassified only with the prior written consent of the originator.

74. In the event that the originator of EUCI cannot be established or traced in respect of documents produced within Parliament, the SA shall review the classification level of the EUCI in question on the basis of a proposal from the parliamentary body/office-holder holding the information, which may consult the CIU in that regard.

75. The CIU or the parliamentary body/office-holder holding the information shall be responsible for notifying the addressee(s) that the information has been declassified or downgraded, and the addressee(s) shall in turn be responsible for notifying any subsequent addressee(s) to whom they have sent or copied the document.

76. The declassification, downgrading or unmarking of information contained in a document shall be recorded.

K.2.Declassification

77. EUCI may be declassified in full or in part. It may be declassified in part when protection is no longer deemed necessary for a specific part of the document containing it but continues to be justified for the rest of the document.

78. When the review of EUCI contained in a document created within Parliament results in a decision to declassify it, consideration shall be given to the question whether the document may be made public or whether it is to bear a distribution marking (i.e. not be made public).

79. When EUCI is declassified, its declassification shall be recorded in the logbook with the following data: date of the declassification, names of the persons who requested and who authorised the declassification, reference number of the declassified document and its final destination.

80. The old classification markings in the declassified document and in all copies thereof shall be struck through. The documents and all copies thereof shall be stored accordingly.

81. Upon partial declassification of classified information, the part that has been declassified shall be produced in the form of an extract and stored appropriately. The competent service shall register:

(a) the date of the partial declassification;

(b) the names of the persons who requested and who authorised the declassification; and

(c) the reference number of the declassified extract.

K.3.Downgrading

82. Following the downgrading of classified information, the document containing it shall be registered in the logbooks corresponding to both the old and the new classification level. The date of downgrading shall be recorded, as well as the name of the person who authorised it.

83. The document containing the downgraded information and all copies thereof shall be classified with the new classification level and stored appropriately.

L.*DESTRUCTION OF CONFIDENTIAL INFORMATION*

84. Confidential information (in either hard copy or electronic form) which is no longer required shall be destroyed or deleted, in accordance with the handling instructions and relevant rules on archiving.

7.3.3.

85. Information classified at the level TRES SECRET UE/EU TOP SECRET or SECRET UE/EU SECRET or its equivalent, shall be destroyed by the CIU. Its destruction shall be witnessed by a person holding security clearance corresponding to at least the classification level of the information being destroyed.

86. Information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent shall be destroyed only with the prior written consent of the originator.

87. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall be destroyed and disposed of by the CIU on instruction from the originator or from a competent authority. The logbooks and other registers shall be updated accordingly. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent shall be destroyed and disposed of either by the CIU or by the relevant parliamentary body/office-holder.

88. The official responsible for the destruction and the person witnessing the destruction shall sign a destruction certificate, to be filed and archived in the CIU. The CIU shall keep, together with the distribution forms, destruction certificates relating to information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent for a period of at least ten years, and, in the case of information classified at the level SECRET UE/EU SECRET or its equivalent and CONFIDENTIEL UE/EU CONFIDENTIAL or its equivalent, for a period of at least five years.

89. Documents containing classified information shall be destroyed by methods which meet the relevant Union standards or equivalent standards so as to prevent them from being reconstructed in whole or in part.

90. The destruction of computer storage media used for classified information shall be carried out in accordance with the relevant handling instructions.

91. Destruction of classified information shall be recorded in the relevant logbook with the following data:

(a) date and time of destruction;

(b) name of the official responsible for destruction;

(c) identification of the document or copies destroyed;

(d) original physical form of the destroyed EUCI;

(e) means of destruction; and

(f) place of destruction.

M.*ARCHIVING*

92. Classified information, including any cover note/letter, annexes, deposit slip and/or other parts of the dossier, shall be transferred to the secure archive in the Secure Area six months after it was last consulted and, at the latest, one year after it was deposited. Detailed rules on the archiving of classified information shall be laid down in the handling instructions.

93. For ‘other confidential information’, the general rules on document management shall apply without prejudice to any other specific provisions on its handling.

7.3.3.

SECURITY NOTICE 3

THE PROCESSING OF CONFIDENTIAL INFORMATION BY MEANS OF AUTOMATED COMMUNICATION INFORMATION SYSTEMS (CIS)

A.*INFORMATION ASSURANCE OF CLASSIFIED INFORMATION HANDLED IN INFORMATION SYSTEMS*

1. 'Information assurance' (IA) in the field of information systems is the confidence that such systems will protect the classified information they handle and will function as they need to and when they need to, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

2. 'Communication Information System' (CIS) for the handling of classified information means a system enabling information to be handled in electronic form. Such an information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources.

3. CIS shall handle classified information in accordance with the concept of IA.

4. CIS shall undergo an accreditation process. Accreditation shall aim at obtaining assurance that all appropriate security measures have been implemented and that a sufficient level of protection of the classified information and of the CIS has been achieved in accordance with this security notice. The accreditation statement shall determine the maximum classification level of the information that may be handled in the CIS as well as the corresponding terms and conditions.

5. The following IA properties and concepts are essential for the security and correct functioning of CIS operations:

(a) authenticity: the guarantee that information is genuine and that it emanates from bona fide sources;

b) availability: the property of being accessible and usable upon request by an authorised entity;

(c) confidentiality: the property that information is not to be disclosed to unauthorised individuals, entities or processes;

(d) integrity: the property of safeguarding the accuracy and completeness of information and assets;

(e) non-repudiation: the ability to prove that an action or event has taken place, so as to preclude the possibility of any subsequent denial of that event or action.

B.*INFORMATION ASSURANCE PRINCIPLES*

6. The provisions set out below shall form the baseline for the security of any CIS handling classified information. Detailed requirements for implementing these provisions shall be defined in IA security policies and security guidelines.

B.1.Security risk management

7. Security risk management shall be an integral part of defining, developing, operating and maintaining CIS. Risk management (assessment, treatment, acceptance and communication) shall be conducted as an iterative process jointly by representatives of the system owners, project authorities, operating authorities and security approval authorities, as laid down in security notice 1, using a proven, transparent and understandable risk assessment process. The

scope of the CIS and its assets shall be clearly defined at the outset of the risk management process.

8. The competent authorities, as laid down in security notice 1, shall review the potential threats to CIS and shall maintain up-to-date and accurate threat assessments which reflect the current operational environment. They shall constantly update their knowledge of vulnerability issues and periodically review the vulnerability assessment to keep up with the changing information technology (IT) environment.

9. The aim of security risk treatment shall be to apply a set of security measures which results in a satisfactory balance between user requirements, cost and residual security risk.

10. Accreditation of a CIS shall include a formal residual risk statement and acceptance of the residual risk by a responsible authority. The specific requirements, scale and degree of detail determined by the relevant SAA for accrediting a CIS shall be commensurate with the risk assessed, taking account of all relevant factors, including the classification level of the classified information handled in the CIS.

B.2.Security throughout the CIS life cycle

11. Ensuring security shall be a requirement throughout the entire CIS life cycle, from initiation to withdrawal from service.

12. The role and interaction of each actor involved in CIS with regard to its security shall be identified for each phase of the life cycle.

13. CIS, including its technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance is obtained and to verify that the CIS, including its technical and non-technical security measures, are correctly implemented, integrated and configured.

14. Security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of CIS and when exceptional circumstances arise.

15. Security documentation for CIS shall evolve over its life cycle as an integral part of the process of change management.

16. Registration procedures performed by a CIS, where required, shall be verified as part of the accreditation process.

B.3.Best practice

17. The IAA shall develop best practice for protecting classified information handled by the CIS. Best practice guidelines shall set out technical, physical, organisational and procedural security measures for CIS with proven effectiveness in countering given threats and vulnerabilities.

18. The protection of classified information handled by the CIS shall draw on lessons learned by entities involved in IA.

19. The dissemination and subsequent implementation of best practice shall help to achieve an equivalent level of assurance for the CIS operated by the Parliament secretariat which handles classified information.

B.4.Defence in depth

20. In order to mitigate risk to CIS, a range of technical and non-technical security measures, organised as multiple layers of defence, shall be implemented. Those layers shall include:

(a) deterrence: security measures aimed at dissuading any adversary planning to attack the CIS;

(b) prevention: security measures aimed at impeding or blocking an attack on the CIS;

(c) detection: security measures aimed at discovering the occurrence of an attack on the CIS;

(d) resilience: security measures aimed at limiting the impact of an attack to a minimum set of information or CIS assets and preventing further damage; and

(e) recovery: security measures aimed at regaining a secure situation for the CIS.

The degree of stringency of such security measures shall be determined following a risk assessment.

21. The competent authorities, as specified in security notice 1, shall ensure that they can respond to incidents which may transcend organisational boundaries in such a way as to coordinate responses and share information about those incidents and the related risks (computer emergency response capabilities).

B.5.Principle of minimalist and least privilege

22. In order to avoid unnecessary risk, only the essential functionalities, devices and services needed to meet operational requirements shall be implemented.

23. CIS users and automated processes shall be given only the access, privileges or authorisations they require in order to perform their tasks, so as to limit any damage resulting from accidents, errors, or unauthorised use of CIS resources.

B.6.Information Assurance awareness

24. Awareness of the risks and available security measures is the first line of defence for the security of CIS. In particular, all personnel involved in the life cycle of CIS, including users, shall understand:

(a) that security failures may significantly harm the CIS handling classified information;

(b) the potential harm to others which may arise from interconnectivity and interdependency; and

(c) their individual responsibility and accountability for the security of CIS according to their roles within the systems and processes.

25. In order to ensure that security responsibilities are understood, IA education and awareness training shall be mandatory for all personal involved, including senior management, Members of the European Parliament and CIS users.

B.7.Evaluation and approval of IT-security products

26. CIS handling information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent shall be protected in such a way that the information cannot be compromised by unintentional electromagnetic emanations (‘TEMPEST security measures’).

27. Where the protection of classified information is provided by cryptographic products, such products shall be certified by the SAA as EU-approved cryptographic products.

28. During transmission of classified information by electronic means, EU-approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures or specific technical configurations may be applied in emergency circumstances as specified in points 41 to 44.

7.3.3.

29. The requisite degree of confidence in the security measures, defined as a level of assurance, shall be determined following the outcome of the risk management process and in line with the relevant security policies and guidelines.

30. The level of assurance shall be verified by using internationally recognised or nationally approved processes and methodologies. This includes primarily evaluation, controls and auditing.

31. The SAA shall approve security guidelines on the qualification and approval of non-cryptographic IT security products.

B.8.Transmission within the Secure Area

32. When transmission of classified information is confined within the Secure Area, unencrypted distribution or encryption at a lower level may be used, based on the outcome of a risk management process and subject to the approval of the SAA.

B.9.Secure interconnection of CIS

33. Interconnection shall mean the direct connection of two or more IT systems for the purpose of sharing data and other information resources in a unidirectional or multidirectional way.

34. CIS shall treat any interconnected IT system as untrustworthy and shall implement protective measures to control the exchange of classified information with any other CIS.

35. For all interconnections of CIS with another IT system the following basic requirements shall be met:

(a) business or operational requirements for such interconnections shall be stated and approved by the competent authorities;

(b) the interconnection in question shall undergo a risk management and accreditation process and shall require the approval of the competent SAA;

(c) protection services (PS) shall be implemented at the perimeter of CIS.

36. There shall be no interconnection between an accredited CIS and an unprotected or public network, except where the CIS has approved PSs installed for such a purpose between the CIS and the unprotected or public network. The security measures for such interconnections shall be reviewed by the competent IAA and approved by the competent SAA.

37. When the unprotected or public network is used solely as a carrier and the data is encrypted by an EU cryptographic product certified in accordance with paragraph 27, such a connection shall not be deemed to be an interconnection.

38. The direct or cascaded interconnection to an unprotected or public network of a CIS accredited to handle information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent or SECRET UE/EU SECRET or its equivalent shall be prohibited.

B.10.Computer storage media

39. Computer storage media shall be destroyed in accordance with procedures approved by the competent security authority.

40. Computer storage media shall be reused, downgraded or declassified in accordance with the handling instructions.

7.3.3.

B.11.Emergency circumstances

41. The specific procedures described below may be applied in an emergency, such as during situations of impending or actual crisis, conflict or war, or in exceptional operational circumstances.

42. Classified information may, with the consent of the competent authority, be transmitted using cryptographic products which have been approved for a lower classification level or without encryption if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:

(a) the sender and the recipient do not have the required encryption facility or have no encryption facility; and

(b) the classified material cannot be conveyed in sufficient time by other means.

43. Classified information transmitted under the circumstances set out in paragraph 41 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

44. Should recourse be had to paragraph 41 or 42 a subsequent report shall be made to the competent authority.

SECURITY NOTICE 4

PHYSICAL SECURITY

A.*INTRODUCTION*

This security notice sets out the security principles for creating a secure environment for ensuring the correct treatment of confidential information in the European Parliament. These principles, including those relating to technical security, will be supplemented by the handling instructions.

B.*SECURITY RISK MANAGEMENT*

1. Risk to classified information shall be managed as a process. That process shall be aimed at determining known security risks, at defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this security notice, and at applying those measures in line with the concept of defence in depth as defined in security notice 3. The effectiveness of such measures shall be continuously evaluated.

2. Security measures for protecting classified information throughout its life cycle shall be commensurate with, in particular, its security classification, the form and volume of the information or material concerned, the location and construction of facilities housing classified information and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

3. Contingency plans shall take account of the need to protect classified information during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability.

4. Preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of classified information shall be included in business continuity plans.

7.3.3.

C.*GENERAL PRINCIPLES*

5. The classification or marking level assigned to the information shall determine the level of protection afforded to it in the areas of physical security.

6. Information which warrants classification shall be marked and handled as such regardless of its physical form. Its classification shall be clearly communicated to its recipients, either by a classification marking (if it is delivered in written form, be it on paper or in CIS) or by an announcement (if it is delivered in oral form, such as in a conversation or a presentation). Classified material shall be physically marked so as to enable its security classification to be easily identified.

7. Confidential information shall not, under any circumstances, be read in public places where it might be seen by an individual without a need to know, e.g. on trains or in planes, cafes, bars etc. It shall not be left in hotel safes or rooms, or left unattended in public places.

D.*RESPONSIBILITIES*

8. The CIU is responsible for ensuring physical security in the management of confidential information deposited in its secure facilities. The CIU is also responsible for the management of its secure facilities.

9. Physical security in the management of information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and of 'other confidential information' is the responsibility of the respective parliamentary body/office-holder.

10. The Directorate for Security and Risk Assessment shall ensure the personal security and security clearance needed to ensure the secure handling of confidential information in the European Parliament.

11. The DIT shall advise and ensure that any created or used CIS is fully in compliance with security notice 3 and the respective handling instructions.

E.*SECURE FACILITIES*

12. Secure facilities may be installed under the technical security standards and in accordance with the level assigned to the confidential information as defined in Article 7.

13. The secure facilities shall be certified by the SAA and validated by the SA.

F.*CONSULTATION OF CONFIDENTIAL INFORMATION*

14. When information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' is deposited with the CIU and has to be consulted outside the Secure Area, the CIU shall transmit a copy to the appropriate authorised service which shall ensure that consultation and handling of the information in question complies with Article 8(2) and Article 10 of this Decision and the appropriate handling instructions.

15. When information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' is deposited with a parliamentary body/office-holder other than the CIU, the secretariat of that parliamentary body/office-holder shall ensure that consultation and handling of the information in question complies with Article 7(3), Article 8(1), (2) and (4), Article 9(3), (4) and (5), Article 10(2) to (6), and Article 11 of this Decision and the appropriate handling instructions.

16. When information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, or its equivalent has to be consulted in the Secure Area, the CIU shall ensure that consultation and handling of the

information in question complies with Articles 9 and 10 of this Decision and the appropriate handling instructions.

G.*TECHNICAL SECURITY*

17. Technical security measures are the responsibility of the SAA, who shall determine in the appropriate handling instructions the specific technical security measures which are to apply.

18. Secure Reading Rooms for consultation of information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and of 'other confidential information' shall comply with specific technical security measures, as provided for in the handling instructions.

19. The Secure Area shall comprise the following facilities:

(a) a Security Access Screening Room (SAS), to be installed in accordance with the technical security measures laid down in the handling instructions. Access to this facility shall be registered. The SAS shall meet high standards in terms of identification of persons with access, video registering, and secure space in which to deposit personal elements that are not allowed in the secured rooms (telephones, pens, etc.);

(b) a communication room for transmission and receipt of classified information, including encrypted classified information, in accordance with security notice 3 and the respective handling instructions;

(c) a secure archive, in which approved and certified containers shall be used separately for information classified at the level RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and/or SECRET EU/EU SECRET or its equivalent. Information classified at the level TRES SECRET UE/EU TOP SECRET or its equivalent shall be placed in a separate room in a specific certified container. The only additional material available in that separate room shall be the support desk for handling the archive by the CIU;

(d) a registry room, which shall provide the tools needed to ensure that registration can be done on paper or electronically and shall thus be equipped with the secure facilities needed for the installation of the appropriate CIS. Only the registry room may contain approved and accredited reproduction devices (for making copies in paper or electronic form). The handling instructions shall specify which reproduction devices are approved and accredited. The registry room shall also provide the space needed in order for accredited material to be stored and handled so as to allow for the marking, copying and dispatching of classified information in physical form, by level of classification. All accredited material shall be defined by the CIU and accredited by the SAA, in accordance with the advice received from the IAOA. The registry room shall also be equipped with the accredited destruction device approved for the highest level of classification, as described in the handling instructions. Translation of information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL EU, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent shall be done in the registry room, in the appropriate and accredited system. The registry room shall provide work stations for up to two translators at a time and for the same document. One staff member of the CIU shall be present;

(e) a reading room, for individual consultation of classified information by duly authorised persons. The reading room shall have enough space for two persons, including a staff member of the CIU who shall be present throughout each consultation. The security level of this room shall be adequate for the consultation of

information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent. The reading room may be equipped with TEMPEST equipment so as to allow for electronic consultation, when needed, in accordance with the level of classification of the information concerned;

(f) a meeting room, which shall be able to accommodate up to 25 persons for the purposes of discussing information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET EU/EU SECRET or its equivalent. The meeting room shall provide the necessary technical secure and certified facilities for interpretation into and out of up to two languages. When not used for meetings, the meeting room may also be used as an additional reading room for individual consultation. In exceptional cases, the CIU may allow more than one authorised person to consult classified information, as long as the level of clearance and the need to know is the same for all persons in the room. No more than four persons shall be allowed to consult classified information at the same time. The presence of CIU officials shall be reinforced;

(g) technical secured rooms for lodging all technical equipment, linked to the security of the entire Secure Area, and the secured IT servers.

20. The Secure Area shall comply with the applicable international security standards and shall be certified by the Directorate for Security and Risk Assessment. The Secure Area shall contain the following minimum security technical equipment:

(a) alarm and monitoring security systems;

(b) safety equipment and emergency systems (two-way warning system);

(c) a CCTV system;

(d) an intrusion detection system;

(e) access control (including a biometric security system);

(f) containers;

(g) lockers;

(h) anti-electromagnetic protection.

21. Where additional technical security measures are needed, these may be added by the SAA, acting in close cooperation with the CIU and with the approval of the SA.

22. The infrastructure equipment may be connected to the general management systems of the building in which the Secure Area is located. However, the security equipment dedicated to access control and to the CIS shall be independent from any other such systems existing within the European Parliament.

H.*INSPECTIONS OF THE SECURE AREA*

23. Inspections of the Secure Area shall be carried out regularly by the SAA and at the request of the CIU.

24. The SAA shall draw up and keep updated the security inspection checklist of items to be verified in the course of an inspection, in line with handling instructions.

7.3.3.

I.*TRANSPORTATION OF CONFIDENTIAL INFORMATION*

25. When carried, confidential information shall be concealed from view and shall give no indication of the confidential nature of its content, in accordance with the handling instructions.

26. Only messengers or staff with the appropriate level of security authorisation may carry information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent.

27. Confidential information may only be despatched by external mail or carried by hand outside a building in accordance with the conditions laid down in the handling instructions.

28. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent shall never be sent by e-mail or fax, even via a 'secure' e-mail system or a crypto-fax machine. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and other confidential information may be send by e-mail using an accredited encryption system.

J.*STORAGE OF CONFIDENTIAL INFORMATION*

29. The classification or marking level assigned to confidential information shall determine the level of protection afforded to it with a view to its storage. It shall be stored in the equipment certified for that purpose, in accordance with the handling instructions.

30. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' shall:

(a) be stored in a standard-issue, steel, locked, cupboard, either within an office or in a working area, when it is not actually being used;

(b) not be left unattended, unless properly locked and stored;

(c) not be left on a desk, table, etc. in such a way that it may be read or removed by any non-authorised individuals, e.g. visitors, cleaners, maintenance personnel, etc.;

(d) not be shown to, or discussed with, any non-authorised individual.

31. Information classified at the level RESTREINT UE/EU RESTRICTED or its equivalent and 'other confidential information' shall be stored only within the secretariats of the parliamentary bodies/office-holders, or in the CIU, in accordance with the handling instructions.

32. Information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET or its equivalent shall:

(a) be stored in the Secure Area, in a security container or in a strongroom. Exceptionally, for example if the CIU is closed, it may be stored in an approved and certified safe deposit within the security services;

(b) not be left unattended within the Secure Area at any time, without first having been locked in an approved safe (even for the briefest of absences);

(c) not be left on a desk, table etc in such a way that it may be read or removed by a non-authorised person, even if the responsible staff member of the CIU remains in the room.

Where a document containing classified information is being produced in electronic form within the Secure Area, the computer shall be locked, and the screen rendered inaccessible if the originator or the responsible staff member of the CIU leaves the room (even for the

briefest of absences). An automatic security lock cutting in after a few minutes shall not be considered a sufficient measure.

SECURITY NOTICE 5

INDUSTRIAL SECURITY

A.*INTRODUCTION*

1. This security notice concerns classified information only.

2. It sets out provisions for implementing the common minimum standards of Part 1 of Annex I to this Decision.

3. 'Industrial security' is the application of measures to ensure the protection of classified information by contractors or subcontractors in pre-contract negotiations and throughout the life cycle of classified contracts. Such contracts shall not involve access to information classified at the level TRÈS SECRET UE/EU TOP SECRET.

4. The European Parliament, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Decision, and referred to in the contract, are complied with when awarding classified contracts to industrial or other entities.

B.*SECURITY ELEMENTS IN A CLASSIFIED CONTRACT*

B.1.Security Classification Guide (SCG)

5. Prior to launching a call for tenders or awarding a classified contract, the European Parliament, as the contracting authority, shall determine the security classification of any information to be provided to bidders and contractors, as well as the security classification of any information to be created by the contractor. For that purpose, it shall prepare a Security Classification Guide (SCG) to be used for the performance of the contract.

6. In order to determine the level of security classification of the various elements of a classified contract, the following principles shall apply:

(a) in preparing an SCG, the European Parliament shall take into account all relevant security aspects, including the security classification assigned to information which is provided and approved by the originator of the information for use in respect of the contract;

(b) the overall level of classification of the contract may not be lower than the highest level of classification of any of its elements.

B.2.Security Aspects Letter (SAL)

7. The contract-specific security requirements shall be described in a Security Aspects Letter (SAL). The SAL shall, where appropriate, contain the SCG and shall be an integral part of a classified contract or sub-contract.

8. The SAL shall contain the provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in this Decision. Non-compliance with those minimum standards may constitute grounds for termination of the contract.

B.3.Programme/Project Security Instructions (PSI)

9. Depending on the scope of programmes or projects involving access to or the handling or storage of EUCI, specific Programme/Project Security Instructions (PSI) may be prepared by the contracting authority designated to manage the programme or project concerned.

7.3.3.

C.*FACILITY SECURITY CLEARANCE (FSC)*

10. An FSC shall be granted by the NSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an industrial or other entity is capable of protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET or its equivalent within its facilities. Evidence of the grant of the FSC shall be presented to the European Parliament, as the contracting authority, before a contractor or subcontractor or potential contractor or subcontractor is provided with, or granted access to, EUCI.

11. An FSC shall:

(a) evaluate the integrity of the industrial or other entity;

(b) evaluate ownership, control, and/or any potential for undue influence that may be considered a security risk;

(c) verify that the industrial or any other entity has established a security system at its facility which covers all appropriate security measures necessary for the protection of information or material classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in accordance with the requirements laid down in this Decision;

(d) verify that the personnel security status of management, owners and employees who are required to have access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has been established in accordance with the requirements laid down in this Decision; and

(e) verify that the industrial or any other entity has appointed a Facility Security Officer who is responsible to its management for enforcing the security obligations within such an entity.

12. Where relevant, the European Parliament, as the contracting authority, shall notify the appropriate NSA or other competent security authority that an FSC is required at the pre-contractual stage or for the performance of the contract. An FSC or Personal Security Clearance (PSC) shall be required at the pre-contractual stage where information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the bidding process.

13. The contracting authority shall not award a classified contract to a preferred bidder until it has received confirmation from an NSA or other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.

14. Any competent security authority which has issued an FSC shall notify the European Parliament, as contracting authority, about any changes affecting that FSC. In the case of a sub-contract, the competent security authority shall be informed accordingly.

15. Withdrawal of an FSC by the relevant NSA or other competent security authority shall constitute sufficient grounds for the European Parliament, as the contracting authority, to terminate a classified contract or exclude a bidder from the competition.

D.*CLASSIFIED CONTRACTS AND SUBCONTRACTS*

16. Where classified information is provided to potential bidders at the pre-contractual stage, the invitation to bid shall contain a provision obliging any of them that fail to submit a bid or that are not selected to return all classified documents within a specified period.

7.3.3.

17. Once a classified contract or subcontract has been awarded, the European Parliament, as the contracting authority, shall notify the NSA of the contractor or subcontractor and/or any other competent security authority about the security provisions of the classified contract.

18. Upon the termination of such a contract, the European Parliament, as the contracting authority (and/or the competent security authority, as appropriate, in the case of a subcontract) shall promptly notify the NSA or any other competent security authority of the Member State in which the contractor or subcontractor is registered.

19. As a general rule, the contractor or subcontractor shall be required, upon termination of the classified contract or subcontract, to return to the contracting authority any classified information held by it.

20. Specific provisions for the disposal of classified information during the performance of the contract or upon its termination shall be laid down in the SAL.

21. Where the contractor or subcontractor is authorised to retain classified information after termination of a contract, the minimum standards contained in this Decision shall continue to apply and the confidentiality of EUCI shall be protected by the contractor or subcontractor.

22. The conditions under which the contractor may subcontract shall be defined in the call for tenders and in the contract.

23. A contractor shall obtain permission from the European Parliament, as the contracting authority, before subcontracting any parts of a classified contract. No subcontract may be awarded to industrial or other entities registered in a third State which has not concluded a security of information agreement with the Union.

24. The contractor shall be responsible for ensuring that all subcontracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.

25. With regard to classified information created or handled by the contractor or subcontractor, the rights vested in the originator shall be exercised by the contracting authority.

E.*VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS*

26. Where the European Parliament, contractors or subcontractors require access to information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract, visits shall be arranged in liaison with the NSAs or any other competent security authority concerned. However, in the context of specific projects, the NSAs may also agree on a procedure whereby such visits can be arranged directly.

27. All visitors shall hold an appropriate PSC and have a ‘need to know’ for access to the classified information related to the European Parliament contract.

28. Visitors shall be given access only to classified information which relates to the purpose of the visit.

F.*TRANSMISSION AND CARRIAGE OF CLASSIFIED INFORMATION*

29. With regard to the transmission of classified information by electronic means, the relevant provisions of security notice 3 shall apply.

30. With regard to the transport of classified information, the relevant provisions of security notice 4 and the relevant handling instructions shall apply.

7.3.3.

31. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

(a) security shall be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) an FSC at the appropriate level shall be obtained for companies providing transportation. In such cases, personnel handling the consignment shall be security cleared in accordance with Annex I;

(d) prior to any cross-border movement of material classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or as SECRET UE/EU SECRET or its equivalent, a transportation plan shall be drawn up by the consignor and approved by the Secretary-General;

(e) journeys shall as far as possible be undertaken from a given point of departure to a given destination point, and shall be completed as quickly as circumstances permit;

(f) the route taken shall wherever possible pass through the territory of Member States.

G.*TRANSFER OF CLASSIFIED INFORMATION TO CONTRACTORS LOCATED IN THIRD STATES*

32. Classified information shall be transferred to contractors and subcontractors located in third States in accordance with security measures agreed between the European Parliament, as the contracting authority, and the third State concerned in which the contractor is registered.

H.*HANDLING AND STORAGE OF INFORMATION CLASSIFIED AT THE LEVEL RESTREINT UE/EU RESTRICTED*

33. In liaison, as appropriate, with the NSA of the Member State concerned, the European Parliament, as the contracting authority, shall be entitled to conduct visits to contractors'/subcontractors' facilities on the basis of contractual provisions in order to verify that the relevant security measures for the protection of EUCI at the level RESTREINT UE/EU RESTRICTED, as required under the contract, have been put in place.

34. To the extent necessary under national laws and regulations, NSAs or any other competent security authorities shall be notified by the European Parliament, as the contracting authority, of contracts or subcontracts containing information classified at the level RESTREINT UE/EU RESTRICTED.

35. An FSC or a PSC for contractors or subcontractors and their personnel shall not be required in the case of contracts awarded by the European Parliament which contain information classified at the level RESTREINT UE/EU RESTRICTED.

36. The European Parliament, as the contracting authority, shall examine the responses to invitations to tender for contracts which require access to information classified at the level RESTREINT UE/EU RESTRICTED, notwithstanding any requirements relating to FSCs or PSCs which may exist under national laws and regulations.

37. The conditions under which the contractor may subcontract shall be defined in the call for tenders and in the contract.

38. Where a contract involves the handling of information classified at the level RESTREINT UE/EU RESTRICTED in communication and information systems operated by a contractor, the European Parliament, as contracting authority, shall ensure that the contract or any

7.3.3.

subcontract specifies the necessary technical and administrative requirements regarding accreditation of the communication and information systems commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation of such communication and information systems shall be agreed between the contracting authority and the relevant NSA.

SECURITY NOTICE 6

BREACHES OF SECURITY, LOSS OR COMPROMISE OF CONFIDENTIAL INFORMATION

1. A breach of security occurs as the result of an act or omission contrary to this Decision which might endanger or compromise confidential information.

2. Compromise of confidential information occurs when it has fallen, wholly or in part, into the hands of unauthorised persons, i.e. persons having neither the appropriate security clearance or the necessary need-to-know, or if the likelihood exists of such an event having occurred.

3. Confidential information may be compromised as a result of carelessness, negligence or indiscretion, as well as by the activities of services which target the Union or of subversive organisations.

4. In the event that the Secretary-General discovers or is informed of a proven or suspected breach of security, loss or compromise relating to confidential information, he/she shall:

(a) establish the facts;

(b) assess and minimise the damage done;

(c) take action to prevent a recurrence;

(d) notify the competent authority of the third party or Member State that originated or forwarded the confidential information.

Where the case concerns a Member of the European Parliament, the Secretary-General shall act in liaison with the President of Parliament.

If the information is received from another Union Institution, the Secretary-General shall act in conformity with the appropriate security measures for classified information and the established arrangements laid down pursuant to the Framework Agreement with the Commission or the Interinstitutional Agreement with the Council.

5. All persons required to handle confidential information shall be thoroughly briefed on security procedures, the dangers of indiscreet conversation and their relationships with the media, and shall, where appropriate, sign a declaration that they will not disclose the contents of confidential information to third persons, that they will respect the obligation to protect classified information and that they acknowledge the consequences of any failure to do so. The access to or use of classified information by a person who has not been briefed and signed the corresponding declaration shall be considered a breach of security.

6. Members of the European Parliament, parliament officials and other Parliament employees working for political groups or contractors shall immediately report to the Secretary-General any breach of security, loss or compromise of confidential information which may come to their notice.

7. Any person responsible for compromising confidential information shall be subject to disciplinary action in accordance with the relevant rules and regulations. Such action shall be without prejudice to any legal action that may be brought pursuant to the applicable law.

7.3.3.

8. Without prejudice to other legal action, breaches committed by Parliament officials and other Parliament employees working for political groups shall entail the application of the procedures and penalties provided for in Title VI of the Staff Regulations.

9. Without prejudice to other legal action, breaches committed by Members of the European Parliament shall be dealt with in accordance with Rule 9(2) and Rules 152, 153 and 154 of Parliament's Rules of Procedure.