College Decision 057/2025

DECISION OF THE COLLEGE OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE OF 18 JUNE 2025

amending the Security Rules of the European Public Prosecutor's Office for the protection of EU Classified Information

The College of the European Public Prosecutor's Office (EPPO),

Having regard to the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), hereinafter referred to as the "EPPO Regulation", and in particular Article 111(2) thereof,

Having regard to Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information, and the need for consistency with those rules, in order to ensure an equivalent level of protection for such information,

Having regard to the Decision of the College of the European Public Prosecutor's Office 011/2021 of 24 February 2021 adopting the Security Rules of the European Public Prosecutor's Office for the Protection of EU Classified Information,

Having regard to the Decision of the College of the European Public Prosecutor's Office 101/2021 of 20 October 2021 amending the Security Rules of the European Public Prosecutor's Office for the Protection of EU Classified Information,

Having regard to Decision of the College of the European Public Prosecutor's Office 014/2024 of 7 February 2024 on Security Rules applicable to The Digital Communication and Information Systems of the European Public Prosecutor's Office ('EPPO'),

Whereas:

(1) The adoption of the Security Rules applicable to The Digital Communication and Information Systems Security of the Communication and Information Systems of the EPPO as well as other relevant developments make it necessary to revise the Security Rules of the EPPO for the protection of EU Classified Information, as contained in College Decision 011/2021 and amended by College Decision 101/2021. For example, the new version should provide for rules on classified meetings.
(2) The revision should also incorporate editorial clarifications and adapt the Security Rules to the current organisational structure of the EPPO. In particular, the European Chief Prosecutor should exercise the capacity of EPPO Security Authority, with the possibility to delegate tasks to the Administrative Director and to EPPO staff.
(3) The new Security Rules should replace the current Security Rules in full, in order to provide a consolidated document of the revised Security Rules. The College should consequently repeal the current Security Rules, which were adopted by College Decision 011/2021 and subsequently amended by College Decision 101/2021.

Has adopted this decision:

Article 1

The Annex to the Decision 011/2021 of the College of the EPPO of 24 February 2021 adopting the Security Rules of the European Public Prosecutor's Office for the protection of EU Classified Information, as amended by the Decision of the College of the European Public Prosecutor's Office 101/2021 of 20 October 2021, is hereby amended and replaced with the Annex to this Decision, which forms an integral part of this Decision.

Article 2

This decision shall enter into force on the day following that of its adoption.

Done at Luxembourg on 18 June 2025.

On behalf of the College,

Laura Codruța KÖVESI

European Chief Prosecutor

Qualified electronic signature by: LAURA CODRUȚA KÖVESI

Date 2025-06-19 09:49:58 UTC

ANNEX:

Security Rules of the European Public Prosecutor's Office for the protection of EU Classified Information

PART I

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

OBJECTIVES

1. These Security Rules implement Article 111(2) of the EPPO Regulation to provide for the appropriate protection of EU classified information (EUCI) processed by the EPPO, consistent with Council Decision 2013/488/EU on the security rules for protecting EU classified information.

SCOPE

2. These Security Rules shall apply to all persons having access to classified information in EPPO, any Communication and Information System or media processing classified information, and all premises and installations containing such information.

Non-compliance may result in disciplinary action in the case of EPPO post-holders or immediate denial of access to EPPO premises for personnel temporarily working at EPPO premises, contractor personnel, including long-term services providers, or visitors.

DEFINITIONS

3. For the purposes of these Security Rules:

(1) "document" means any recorded information regardless of its physical form or characteristics.

(2) "material" means any document and also any item of equipment or asset;

(3) "case-related information" means any information linked to the operational tasks of EPPO, as defined in Article 4 of the EPPO Regulation[1];
(4) "EU classified information" (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or one or more of its Member States;
(5) "personal data" means any information relating to an identified or identifiable natural person ("data subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
(6) "need-to-know" means the need of an individual to have access to EUCI in order to be able to perform a function or task;
(7) "originator" means the issuing party of EUCI;
(8) "post-holder" means the persons defined in the Glossary of Administrative terms and Abbreviations, Version 2.0[2];
(9) "National Security Authority" (NSA) means: The government authority of each EU member state with ultimate responsibility for the protection of classified information.
(10) "Transmission" means the transfer of a signal, message, or other form of information from one location to another.
(11) "Distribution" means any process, either electronic or otherwise, for transmitting EUCI to post-holders, national authorities, partners, Third States, international organisations or others.
(12) "Dissemination of information" means the disclosure of information by any means to a wider audience by means of e-mail, seminars, newsletters, press releases, memos and similar methods.
(13) "Downgrading" means a reduction in the level of classification as referred to in Part II, Section II.
(14) "Declassification" means the removal of any classification as referred to in Part II, Section II.
(15) "Confidentiality" means ensuring that information is accessible only to those authorised to have access.

[1] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')
[2] Decision EPPO/2023/AD/160 of the Administrative Director of the EPPO of 4 June 2023 updating EPPO's Glossary of Administrative Terms and Abbreviations (Ref. Ares (2023)4131648 – 14/06/2023).

(16) "Availability" means that access is ensured to those needing and authorised to have access to information, and especially to information stored, further processed or transmitted in electromagnetic form.

(17) "Authenticity" means the guarantee that information is genuine and from bona fide sources.

(18) "Non-repudiation" means the ability to prove an action or event has taken place, so that this event or action cannot be denied.

(19) "Integrity" means the prevention of corruption, unauthorised alteration or unauthorised deletion of information.

(20) "Breach of security" means the result of any act or omission contrary to these Security Rules which compromises EUCI. Compromise of EUCI occurs when such information has, in whole or in part, fallen into the hands of unauthorised persons who have neither the appropriate security clearance nor the necessary need-to-know or when there is the likelihood of such an event having occurred.

(21) "Defence in depth" means the application of a range of security measures organised as multiple layers of defence.

(22) 'Facility Security Clearance' (FSC) means an administrative determination by a NSA, DSA or any other competent security authority that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI to a specified security classification level.

(23) 'Personnel Security Clearance' (PSC) means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date.

(24) "Registration for security purposes (registration)" means the application of procedures which record the life-cycle of EUCI including its dissemination and destruction.

(25) "Information Assurance" means the confidence that communication and information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

(26) "Communication and Information System" means any system enabling the handling of EUCI in electronic form and is comprised of all assets required for it to operate, including the infrastructure, organisation, personnel and information resources.

(27) "Interconnection" means the direct connection of two or more IT systems for the purpose of sharing data and other information resources (e.g. communication) in a unidirectional or multidirectional way.

(28) "Security Classification Guide (SCG)" means a document which describes the elements of a programme or contract which are classified, specifying the applicable security classification levels.

(29) "Designated Security Authority" (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority.

(30) "Long-term service provider" means the persons defined in the Glossary of Administrative terms and Abbreviations, Version 2.0[3].

CLASSIFICATION MARKINGS

4. EUCI shall be clearly identified as classified information, and retain its classification level for only as long as necessary.

5. EUCI shall not be downgraded or declassified nor shall any of the classification markings be modified or removed without the prior demonstrable consent of the originator.

PROTECTION OF CLASSIFIED INFORMATION

6. EPPO post-holders who are in possession of any item of EUCI shall be responsible for protecting it in accordance with these Security Rules.

7. Where Member States transferred classified information bearing a national security classification marking into the structures or networks to the EPPO, the EPPO shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Appendix 1.

[3] Decision EPPO/2023/AD/160 of the Administrative Director of the EPPO of 4 June 2023 updating EPPO's Glossary of Administrative Terms and Abbreviations (Ref. Ares (2023)4131648 – 14/06/2023).

SECURITY RISK MANAGEMENT

8. Risk to EUCI shall be managed as a process. This process shall be aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in these Security Rules and at applying these measures in line with the concept of defence in depth. The effectiveness of such measures shall be continuously evaluated.

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

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

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

CONFIDENTIALITY AND CLASSIFICATION

12. Where confidentiality is concerned, care and experience are needed in the selection of information and material to be protected and the assessment of the degree of protection required. It is fundamental that the degree of protection shall correspond to the security classification of the individual piece of information or material to be protected. In order to ensure the smooth flow of information, steps shall be taken to avoid both over- and under-classification.

PERSONNEL SECURITY

13. Personnel security measures shall be applied at the EPPO to ensure that access to EUCI is granted only to persons who have:

a) a need to know,

b) been security cleared to the relevant level, where appropriate, and

c) been briefed on their responsibilities.

14. Personnel security clearance procedures shall be carried out in accordance with Article 7 and Annex I of Council Decision 2013/488/EU on the security rules for protecting EU classified information in order to determine whether a person, taking into account their loyalty, trustworthiness and reliability, may be authorised to access EUCI.

15. All post-holders and long-term service providers whose duties require them to have access to or handle EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level before being granted access to such EUCI. Such persons shall be authorised by the EPPO Security Authority to access EUCI up to a specified level and up to a specified date. Security clearance shall also be required for post-holders or long-term service providers whose duties involve the technical operation or maintenance of communication and information systems containing or processing EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above.

16. The number of EPPO post-holders and long-term service providers authorised to originate TRÈS SECRET UE/EU TOP SECRET documents shall be kept to a minimum, and their names kept on a list drawn up by the Head of Security Unit.

17. By virtue of their function and in accordance with Articles 11, 12 and 13 of the EPPO Regulation, the European Chief Prosecutor, the Deputy European Chief Prosecutors, the European Prosecutors and the European Delegated Prosecutors shall be empowered to exchange any classified information necessary for the performance of the tasks of EPPO, without a PSC, among themselves or with their Member States' competent authorities, without prejudice to otherwise existing obligations concerning the exchange of classified information.

18. For reasons of urgency, where duly justified in the interests of the service and pending the completion of the security clearance process, the EPPO Security Authority may, after consulting the NSA of the Member State of whom the person is a national and subject to the outcome of preliminary checks to verify that no adverse information is known, grant a temporary authorisation for post-holders to access EUCI for a specific function. Long-term service providers may not be granted a temporary authorisation.

Such temporary authorisations shall be valid for a period not exceeding 6 months and shall not permit access to information classified TRÈS SECRET UE/EU TOP SECRET. All persons who

have been granted a temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Security Unit.

19. The Administrative Director, for post-holders directly reporting to him or her, and the Heads of Units, for post-holders working in the respective unit, shall have the duty of knowing which post-holders are authorised to access EUCI. To this end, the EPPO Security Unit shall maintain a list of all post-holders and long-term service providers that are authorised to access EUCI. The EPPO Security Unit shall inform each line manager of any update related to this topic in regards to post-holders and long-term service providers reporting to them.

20. Before being granted access to EUCI and at regular intervals thereafter, all post-holders and long-term service providers shall be briefed on and acknowledge their responsibilities to protect EUCI in accordance with these Security Rules. A record of such briefings and written acknowledgement shall be kept by the EPPO Security Unit.

21. Persons not having a need-to-know, such as couriers, guards, escorts, maintenance personnel and cleaners, but who may have access to EUCI shall be security cleared to the relevant level or otherwise appropriately investigated in accordance with national laws and regulations, be briefed on security procedures for protecting EUCI and be instructed on their duties for protecting such information.

PHYSICAL SECURITY

22. The EPPO shall put in place physical and technical protective measures to prevent unauthorised access to EUCI.

23. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow for segregation of personnel in their access to EUCI on a need-to-know basis. Such measures shall be determined based on a risk management process.

24. Physical security measures shall be put in place for all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems.

25. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with Part II, Section IV. The approval of Secured Areas may be delegated to the EPPO Security Unit.

26. Only approved equipment or devices shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

27. Provisions for implementing physical security measures are set out in Part II, Section IV.

MANAGEMENT OF CLASSIFIED INFORMATION

28. Administrative measures for managing EUCI throughout its life-cycle shall be put in place to help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, downgrading, declassification, carriage and destruction of EUCI.

29. Classified information, other than EUCI, shall be managed in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Appendix 1.

30. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt in the logbook maintained by the EPPO Registry for this purpose. Information classified TRÈS SECRET UE/EU TOP SECRET shall be registered in the EPPO TRÈS SECRET UE/EU TOP SECRET Registry.

31. Services and premises where EUCI is handled or stored shall be subject to inspection by the Council Secretariat Security Office with assistance from experts of the Luxembourg NSA as defined in Council Decision 2013/488/EU on the security rules for protecting EU classified information.

32. Provisions for implementing the management of EUCI are set out in Part II, Section III.

PROTECTION OF EUCI HANDLED IN COMMUNICATIONS AND INFORMATION SYSTEMS

33. These security rules shall apply to communication and information systems (CIS) handling EUCI.

34. All CIS at EPPO that handle EUCI shall do so in accordance with the concept of information assurance (IA) in order to ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. The IA measures shall be based on a risk management process.

35. All CIS at EPPO that handles EUCI 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 EUCI and of the CIS has been achieved in accordance with these Security Rules. The accreditation statement shall determine the maximum classification level of the information that may be handled in a CIS as well as the corresponding terms and conditions.

36. Security measures shall be implemented to protect CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above against compromise of such information through unintentional electromagnetic emanations ("TEMPEST security measures"). Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information.

37. Where the protection of EUCI is provided by cryptographic products, such products shall be approved by the Council or the Secretary-General of the Council in accordance with Article 10(6) of Council Decision 2013/488/EU on the security rules for protecting EU classified information.

38. [deleted]

39. During transmission of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances.

40. The following Information assurance functions shall be established at EPPO:

a) The function of Information Assurance Authority (IAA), as described in section VII, paragraph 209

Shall be assigned to the EPPO Security Authority;

b) the function of TEMPEST Authority, as described in section VII, paragraph 210

Shall be assigned the EPPO Security Authority;

c) the function of crypto distribution authority (CDA), as described in section VII, paragraph 211

Shall be assigned to the Head of Security Unit;

d) the function of Security Accreditation Authority (SAA), as described in section VII, paragraph 212

Shall be assigned to the EPPO Security Authority;

e) The function of Information Assurance Operational Authority (IAOA), as described in section VII, Paragraph 213

Shall be assigned to the Head of Security Unit.

INDUSTRIAL SECURITY

41. Security measures shall be applied to ensure the protection of EUCI by private parties in pre-contract negotiations and throughout the life-cycle of classified contracts let by EPPO and in subcontracts let by EPPO prime contractors. Such contracts shall not involve access to information classified TRÈS SECRET UE/EU TOP SECRET.

42. The EPPO, as contracting authority, shall ensure that the minimum standards on industrial security set out in these Security Rules are referred to in the contract and are complied with when awarding classified contracts to industrial or other entities.

43. The EPPO shall as far as possible ensure, in cooperation with NSA, DSA or any other competent national security authorities, and in accordance with national laws and regulations, that contractors or subcontractors registered in the respective Member State participating in classified contracts or sub-contracts which require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either in the performance of such contracts or during the pre-contractual stage, hold a Facility Security Clearance (FSC) at the relevant classification level.

44. Contractor or subcontractor personnel who, for the performance of a classified contract, require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be granted a Personnel Security Clearance (PSC) by the respective NSA, DSA or any other competent security authority in accordance with national laws and regulations and the minimum standards laid down in Annex I of Council Decision 2013/488/EU on the security rules for protecting EU classified information.

45. Provisions for implementing these provisions about industrial security are set out in Section VIII of these Security Rules.

SHARING EUCI WITH OTHER UNION INSTITUTION, BODIES OR AGENCIES

46. To exchange EUCI with other EU IBOAs, dedicated arrangements may be concluded at the discretion of the College. Any such arrangements shall ensure that EUCI is given protection appropriate to its classification level and according to basic principles and minimum standards which shall be equivalent to those laid down in these Security Rules. If EUCI to be shared does not originate in the EPPO, the originator's consent shall be obtained prior to the sharing.

47. In the absence of such an arrangement, EUCI may only be shared where this is exceptionally necessary in individual and concrete cases, and after the European Chief Prosecutor has provided assent to such sharing. The European Chief Prosecutor's decision shall take into account the recommendation from the Head of Security Unit. The decision and the recommendation shall consider the circumstances of the case and the level of protection likely to be provided to the information by the recipient as well as the intended manner of transfer and the risks stemming from unintended disclosure of the EUCI.

EXCHANGE OF CLASSIFIED INFORMATION WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

48. Provided that the European Union has concluded an agreement on exchanging and protecting classified information with the third State or international organisation and that the EPPO had identified a long-term need to exchange classified information with the authorities of that third State or international organisation, an appropriate framework shall be put in place to that effect.

49. This may be part of any working arrangement concluded with the recipient in line with Article 99(3) of the EPPO Regulation or take the form of a separate or dedicated implementing instrument.

50. Any arrangements referred to in previous paragraph shall be based upon a model arrangement approved by the College, and contain provisions to ensure that when the authorities of third states or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are no less stringent than those laid down in these Security Rules.

The decision to release EUCI originating in the EPPO to the authorities of a third State or international organisation shall be taken by the EPPO on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the Union. If the originator of the classified information for which release is desired is not the EPPO, the EPPO shall first seek the originator's written consent to release. If the originator cannot be established, the EPPO shall assume the former's responsibility.

51. Where appropriate, assessment visits by the EPPO may be arranged to ascertain the effectiveness of the security measures in place in the authorities of a third State or international organisation for protecting EUCI provided or exchanged.

52. In the absence of an arrangement referred to in point 49,

a) The exchange of EUCI may occur mutatis mutandis to the provisions of Article 104(5) of the EPPO Regulation as regards the utilisation of instruments available under respective national law allowing for the exchange of EUCI or its equivalent on national level.

b) Or, alternatively and only if necessary in individual and concrete cases, and after the European Chief Prosecutor has provided assent to such a release. The European Chief Prosecutor's assent decision has to be based on the recommendation from the Head of Security Unit, having taken into account the circumstances of the case and the level of protection likely to be provided to the information by the recipient as well as the intended manner of transfer, and the risks stemming from unintended disclosure of the EUCI.

PART II

SECTION I: THE ORGANISATION OF SECURITY AT EPPO

53. The **College** shall:

a) be responsible for approving these Security Rules; and
b) decide on the specific issues mentioned in paragraph 200 of these Security Rules.

54. The **European Chief Prosecutor** shall be the EPPO Security Authority. In the capacity of Security Authority he/she shall:

a) ensure the implementation and update of these Security Rules;
b) examine all security-related issues involving changes in these Security Rules, in close liaison with the NSA and the relevant Security Authorities where necessary;
c) perform the function of the Information Assurance Authority, the TEMPEST Authority, and the Security Accreditation Authority,
d) perform the specific functions mentioned in these Security Rules;
e) propose amendments to these Security Rules to the College of EPPO whenever appropriate;
f) grant post-holders authorisation for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above; and
g) ensure that security breaches are appropriately dealt with and reported as appropriate;
h) investigate or order an investigation into any leakage of EUCI which, on prima facie evidence, has occurred in the EPPO;
i) request the appropriate authorities to initiate investigations when a leakage of EUCI appears to have occurred outside the EPPO, and co-ordinating the enquiries when more than one authority is involved;
j) ensure the periodic inspections of the security arrangements for protecting classified information on EPPO premises;
k) carry out jointly, and in agreement with the authority concerned, periodic assessment visits of the security arrangements for the protection of classified information within third states or international organisations in agreement with the authority concerned;
l) enter into working arrangements in line with the principles and process described by these Security Rules;
m) keep the College informed of any relevant security developments.

With the exception of points d) and h), the European Chief Prosecutor may delegate responsibilities of the EPPO Security Authority to the **Administrative Director**. The Administrative Director may sub-delegate responsibilities to the Head of Security Unit.[4]

55. The EPPO **Security Unit** shall:

a) assist the Security Authority and the Head of Security Unit in fulfilling the responsibilities mentioned in these Security Rules ;
b) maintain close liaison with all security authorities concerned in order to achieve overall co-ordination of security; and
c) perform the specific functions mentioned in these Security Rules.

56. The **Head of Security Unit** shall:

a) advise and assist the Security Authority and the Administrative Director on the implementation of these Security Rules and any other security matter;
b) co-ordinate security measures with the competent authorities of the Member States, third states and international organisations in case of threats or incidents affecting physical integrity of persons, premises or other assets in EPPO;
c) continuously monitor threats and risks to security;
d) ensure the accreditation of IT systems and networks within EPPO;
e) supervise and carry out the day-to-day implementation of these Security Rules and procedures;
f) co-ordinate the security clearance procedure;
g) make enquiries and checks as may be necessary to ensure that the Security Rules, procedures and measures are implemented;
h) assist and advise the Security Authority and other post-holders in all matters relating to security, and, in particular, issuing detailed instructions for the implementation of these Security Rules where appropriate;
i) investigate breaches of these Security Rules and report them in accordance with Section VI of these Security Rules;
j) consider any ways in which security might be improved;
k) instruct post-holders on their duties regarding the application of security measures;
l) keep an up-to-date list of all persons who are authorised to have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above;

[4] E.g. Signature of the security authorisations to access EUCI

m) keep an up-to-date list of all registers as defined in these Security Rules;
n) make enquiries and checks as may be necessary to ensure that the registers are kept in accordance with the applicable provisions of these rules;
o) act as Crypto Distribution Authority and Information Assurance Operational Authority; and
p) act as a Chief Registry Officer in relation to the procedure for registration of EUCI at EPPO.

SECTION II: CLASSIFICATIONS AND MARKINGS

LEVELS OF CLASSIFICATION

57. Information is classified at the following levels:

a) TRÈS SECRET UE/EU TOP SECRET: this classification shall be applied only to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union, or of one or more of its Member States,

b) SECRET UE/EU SECRET: this classification shall be applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union, or of one or more of its Member States,

c) CONFIDENTIEL UE/EU CONFIDENTIAL: this classification shall be applied to information and material the unauthorised disclosure of which could harm the essential interests of the European Union, or of one or more of its Member States,

d) RESTREINT UE/EU RESTRICTED: this classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union, or of one or more of its Member States.

A comparative table of national security classifications may be found in Appendix 1.

CAVEAT MARKINGS

58. A caveat marking may be used for specifying the field covered by the document or a particular distribution on a need-to-know basis.

AFFIXING OF CLASSIFICATION AND MARKINGS

59. Classification and markings shall be applied as follows:

a) on RESTREINT UE/EU RESTRICTED documents, by mechanical or electronic means,
b) on CONFIDENTIEL UE/EU CONFIDENTIAL documents, by mechanical means and by hand or by printing on pre-stamped registered paper, and

c) on SECRET UE/EU SECRET and TRÈS SECRET UE/EU TOP SECRET documents, by mechanical means and by hand.

SECTION III: MANAGEMENT OF CLASSIFIED INFORMATION

INTRODUCTION

60. This Section sets out provisions for implementing the management of EUCI. It lays down the administrative measures for controlling EUCI throughout its life-cycle in order to help deter and detect deliberate or accidental compromise or loss of such information.

CLASSIFICATION MANAGEMENT

Classifications and markings

61. Information shall be classified where it requires protection with regard to its confidentiality.

62. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant classification guidelines, and for the initial dissemination of the information.

63. The classification level of EUCI shall be determined in accordance with these Security Rules.

64. The security classification shall be clearly indicated, regardless of whether the EUCI is on paper, oral, electronic or in any other form.

65. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and shall be marked accordingly, including when stored in electronic form.

66. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. 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 than its component parts.

67. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.

68. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:

CONFIDENTIEL UE/EU CONFIDENTIAL

Without attachment(s) RESTREINT UE/EU RESTRICTED

Markings

69. In addition to one of the security classification markings set out in Part II, Section II of these Security Rules, EUCI may bear additional markings, such as:

a) an identifier to designate the originator;

b) any caveats, code-words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use;

c) releasability markings; or

d) where applicable, the date or specific event after which it may be downgraded or declassified.

Abbreviated classification markings

70. Standardised abbreviated classification markings may be used to indicate the classification level of individual paragraphs of a text. Abbreviations shall not replace the full classification markings.

71. The following standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page:

a)TRÈS SECRET UE/EU TOP SECRET | TS-UE/EU-TS |

b) SECRET UE/EU SECRET | S-UE/EU-S |

c) CONFIDENTIEL UE/EU CONFIDENTIAL | C-UE/EU-C |

d) RESTREINT UE/EU RESTRICTED | R-UE/EU-R |

Creation of EUCI

72. When creating an EU classified document:

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

b) each page shall be numbered;

c) the document shall bear a reference number and a subject, which is not itself classified information, unless it is marked as such;

d) the document shall be dated; and

e) documents classified SECRET UE/EU SECRET or above shall bear a copy number on every page, if they are to be distributed in several copies.

73. The originator of an EUCI shall not over- or under-classify.

Downgrading and declassification of EUCI

74. At the time of its creation, the originator shall indicate, where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether EUCI can be downgraded or declassified on a given date or following a specific event.

75. The EPPO shall regularly review EUCI held by it to ascertain whether the classification level still applies. The EPPO shall establish a system to review the classification level of EUCI which it has originated no less frequently than every five years. Such a review shall not be necessary where it has been indicated from the outset that the information will automatically be downgraded or declassified and the information has been marked accordingly.

REGISTRATION OF EUCI FOR SECURITY PURPOSES

76. The EPPO Registry shall be established to ensure that EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL and above is handled in accordance with these Security Rules. The EPPO Registry shall be established as a Secured Area, as defined in Part II, Section IV of these Security Rules.

77. All information and material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above, or at an equivalent level as set out in the table of equivalence of security classifications contained in Appendix 1, shall be registered by the EPPO Registry when they are received at or sent by the EPPO.

78. The EPPO Registry shall keep a record of all EUCI released by EPPO to third states and international organisations, and of all classified information received from third states or international organisations.

79. In the case of a CIS, registration procedures may be performed by processes within the CIS itself.

80. A procedure on the registration of EUCI for security purposes shall be established.

The EPPO TRÈS SECRET UE/EU TOP SECRET Registry

81. The EPPO TRÈS SECRET UE/EU TOP SECRET Registry shall be established to ensure that EUCI classified TRÈS SECRET UE/EU TOP SECRET is handled in accordance with these Security Rules.

82. The EPPO TRÈS SECRET UE/EU TOP SECRET Registry shall act as the central receiving and dispatching authority for information classified TRÈS SECRET UE/EU TOP SECRET.

COPYING AND TRANSLATING EU CLASSIFIED DOCUMENTS

83. TRÈS SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.

84. Where the originator of documents classified SECRET UE/EU SECRET and below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder of the document.

85. The security measures applicable to the original document shall apply to copies and translations thereof.

CARRIAGE OF EUCI

86. Carriage of EUCI shall be subject to the protective measures set out in paragraphs 86 to 100.

87. EUCI carried on electronic media shall be protected by cryptographic products approved in accordance with these Security Rules or as prescribed by the Head of Security Unit in accordance with the relevant protection measures laid down in this Section.

88. The Head of Security Unit shall issue instructions on the carriage of EUCI in accordance with these Security Rules.

Within a building or self-contained group of buildings

89. EUCI carried within a building or self-contained group of buildings shall be covered in order to prevent observation of its contents.

90. Within a building or self-contained group of buildings, information classified TRÈS SECRET UE/EU TOP SECRET shall be carried in a secured envelope bearing only the addressee's name.

Within the Union

91. EUCI carried between buildings or premises within the Union shall be packaged so that it is protected from unauthorised disclosure.

92. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within the Union shall be by one of the following means:

a) military, government or diplomatic courier, as appropriate;

b) hand carriage, provided that:

i. EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Section IV;

ii. EUCI is not opened en route or read in public places;

iii. persons are briefed on their security responsibilities; and

iv. persons are provided with a courier certificate where necessary;

c) postal services or commercial courier services, provided that:

i. they are approved by the relevant NSA in accordance with national laws and regulations; and

ii. they apply appropriate protective measures in accordance with minimum requirements to be laid down in security guidelines developed by the Security Committee of the Council in accordance with Article 6(2) of Council Decision 2013/488/EU on the security rules for protecting EU classified information.

In the case of carriage from one Member State to another, the provisions of point (c) shall be limited to information classified up to CONFIDENTIEL UE/EU CONFIDENTIAL.

93. Information classified RESTREINT UE/EU RESTRICTED may also be carried by postal services or commercial courier services. A courier certificate is not required for the carriage of such information.

94. Material classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET (e.g. equipment or machinery) which cannot be carried by the means referred to in paragraph 92 shall be transported as freight by commercial carrier companies in accordance with Part II, Section VIII of these Security Rules.

95. The carriage of information classified TRÈS SECRET UE/EU TOP SECRET between buildings or premises within the Union shall be by military, government or diplomatic courier, as appropriate.

From within the Union to the territory of a third state

96. EUCI carried from within the Union to the territory of a third state shall be packaged in such a way that it is protected from unauthorised disclosure.

97. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from within the Union to the territory of a third state shall be by one of the following means:

a) military or diplomatic courier;

b) hand carriage, provided that:

i. the package bears an official seal, or is packaged so as to indicate that it is an official consignment and should not undergo customs or security scrutiny;

ii. persons carry a courier certificate identifying the package and authorising them to carry the package;

iii. EUCI does not leave the possession of the bearer, unless it is stored in accordance with the requirements set out in Part II, Section IV of these Security Rules;

iv. EUCI is not opened en route or read in public places; and

v. persons are briefed on their security responsibilities.

98. The carriage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET released by EPPO to a third state or international organisation shall comply with the relevant provisions under a security of information Agreement or an administrative arrangement in accordance with Part I, paragraph 52 (a) or (b) of these Security Rules.

99. Information classified RESTREINT UE/EU RESTRICTED may also be carried by postal services or commercial courier services.

100. The carriage of information classified TRÈS SECRET UE/EU TOP SECRET from within the Union to the territory of a third state shall be by military or diplomatic courier.

DESTRUCTION OF EUCI

101. EUCI documents which are no longer required must be destroyed, without prejudice to the relevant rules and regulations on archiving. Post-holders who keep EUCI shall review it on an annual basis to assess whether they need to keep it longer. If it is not necessary for post-holders to keep it longer, they shall then destroy it immediately.

102. Documents subject to registration in accordance with Part I, paragraph 29 of these Security Rules shall be destroyed by the EPPO Registry on instruction from the holder or from a competent authority. The logbooks and other registration information shall be updated accordingly.

103. For documents classified SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET, destruction shall be performed in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.

104. The register officer and the witness, where the presence of the latter is required, shall sign a destruction certificate, which shall be filed in the EPPO Registry. The EPPO Registry shall keep destruction certificates of TRÈS SECRET UE/EU TOP SECRET documents for a period of at least 10 years and of documents CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET for a period of at least five years.

105. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which meet relevant Union or equivalent standards or which have been approved by Member States in accordance with national technical standards so as to prevent reconstruction in whole or in part.

106. The destruction of computer storage media used for EUCI shall be in accordance with the provisions for the highest level of classification for which the storage media was used.

107. In the event of an emergency, if there is an imminent risk of unauthorised disclosure EUCI shall be destroyed by the holder in such a way that it cannot be reconstructed in whole or in part. The originator and originating registry shall be informed of the emergency destruction of registered EUCI.

SECTION IV: PHYSICAL SECURITY

INTRODUCTION

108. This Section sets out provisions for implementing Part I, paragraphs 22-27 on physical security. It lays down minimum requirements for the physical protection of premises, buildings, offices, rooms and other areas where EUCI is handled and stored, including areas housing CIS.

109. Physical security measures shall be designed to prevent unauthorised access to EUCI by:

a) ensuring that EUCI is handled and stored in an appropriate manner;

b) allowing for segregation of post-holders in terms of access to EUCI on the basis of their need-to-know and, where appropriate, their security clearance;

c) deterring, impeding and detecting unauthorised actions; and

d) denying or delaying surreptitious or forced entry by intruders.

PHYSICAL SECURITY REQUIREMENTS AND MEASURES

110. Physical security measures shall be selected on the basis of a threat assessment made by the competent authorities. The EPPO shall apply a risk management process for protecting EUCI on its premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. The risk management process shall take account of all relevant factors, in particular:

a) the classification level of EUCI;

b) the form and volume of EUCI, bearing in mind that large quantities or a compilation of EUCI may require more stringent protective measures to be applied;

c) the surrounding environment and structure of the buildings or areas housing EUCI; and

d) the assessed threat from intelligence services which target the Union or Member States and from sabotage, terrorist, subversive or other criminal activities.

111. The EPPO, applying the concept of defence in depth, shall determine and deploy the appropriate combination of physical security measures. These can include one or more of the following:

a) a perimeter barrier: a physical barrier which defends the boundary of an area requiring protection;

b) intrusion detection systems (IDS): an IDS may be used to enhance the level of security offered by a perimeter barrier, or in rooms and buildings in place of, or to assist, security staff;

c) access control: access control may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. Control may be exercised by electronic or electro-mechanical means, by security personnel and/or a receptionist, or by any other physical means;

d) security personnel: trained, supervised and, where necessary, appropriately security-cleared security personnel may be employed, inter alia, in order to deter persons planning covert intrusion;

e) closed circuit television (CCTV): CCTV may be used by security personnel in order to verify incidents and IDS alarms on large sites or at perimeters;

f) security lighting: security lighting may be used to deter a potential intruder, as well as to provide the illumination necessary for effective surveillance directly by security personnel or indirectly through a CCTV system; and

g) any other appropriate physical measures designed to deter or detect unauthorised access or prevent loss of or damage to EUCI.

112. When EUCI is at risk of being observed by others, even accidentally, appropriate measures shall be taken to counter this risk.

113. For new facilities, physical security requirements and their functional specifications shall be defined as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented to the maximum extent possible.

EQUIPMENT FOR THE PHYSICAL PROTECTION OF EUCI

114. When acquiring equipment (such as security containers, shredding machines, door locks, electronic access control systems, IDS, alarm systems) for the physical protection of EUCI, the EPPO Security Unit shall ensure that the equipment meets approved technical standards and minimum requirements.

115. The EPPO Security Unit shall maintain an up-to-date list by type and model of the security equipment which is approved for the direct or indirect protection of EUCI under various specified circumstances and conditions, based, inter alia, on information from the General Secretariat of the Council and, as appropriate, from the NSA of its host Member State.

116. When electrical devices are used to protect EUCI, an emergency electrical supply shall be available to ensure the continuous operation of the system if the main power supply is interrupted. A malfunction in or tampering with such systems shall result in an alarm or other reliable warning to the surveillance personnel.

117. Security systems shall be inspected at regular intervals and equipment shall be maintained regularly. Maintenance work shall take account of the outcome of inspections to ensure that equipment continues to operate at optimum performance.

118. The effectiveness of individual security measures and of the overall security system shall be re-evaluated during each inspection.

PHYSICALLY PROTECTED AREAS

119. Two types of physically protected areas shall be established for the physical protection of EUCI:

a) Administrative Areas; and

b) Secured Areas (including technically Secured Areas).

120. Before an area is designated as an Administrative Area, a Secured Area or a technically Secured Area, an assessment shall be carried by the EPPO Security Unit certifying that the necessary physical security requirements are met.

121. For Administrative Areas:

a) a visibly defined perimeter shall be established which allows persons and, where possible, vehicles to be checked;

b) unescorted access shall be granted only to post-holders and long-term service providers who are duly authorised and

c) all other persons shall be escorted at all times or be subject to equivalent controls.

122. For Secured Areas:

a) a visibly defined and protected perimeter shall be established through which all entry and exit are controlled by means of a pass or personal recognition system;

b) unescorted access shall be granted only to post-holders and long-term service providers who are security-cleared and specifically authorised to enter the area on the basis of their need-to-know; and

c) all other persons shall be escorted at all times or be subject to equivalent controls.

123. Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, the following additional requirements shall apply:

a) the level of highest security classification of the information normally held in the area shall be clearly indicated;

b) all visitors shall require specific authorisation to enter the area, shall be escorted at all times and shall be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible.

124. Secured Areas protected against eavesdropping shall be designated technically Secured Areas. The following additional requirements shall apply:

a) such areas shall be IDS equipped, be locked when not occupied and be guarded when occupied. Any keys shall be controlled in accordance with this Section;

b) all persons and material entering such areas shall be controlled;

c) such areas shall be regularly physically and/or technically inspected as required by the competent security authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry;

d) such areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment;

e) a detailed inventory of equipment and furniture in such areas shall be kept. No item of furniture or equipment shall be brought into such an area until it has undergone a careful inspection by specially trained security personnel, designed to detect any listening devices.

125. Notwithstanding point (d) of paragraph 124, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET and above, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined by the EPPO Security Unit to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area. If necessary, such devices may be checked by technical security specialists at the request of the Head of Security Unit.

126. Secured Areas which are not occupied by duty personnel on a 24-hour basis shall, where appropriate, be inspected at the end of normal working hours and at random intervals outside normal working hours, unless an IDS is in place.

127. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.

128. Security operating procedures shall be drawn up for each Secured Area stipulating:

a) the level of EUCI which may be handled and stored in the area;

b) the surveillance and protective measures to be maintained;

c) the post-holders and visitors authorised to have unescorted access to the area by virtue of their need-to-know and security clearance;

d) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other persons to access the area; and

e) any other relevant measures and procedures.

129. Strong rooms shall be constructed within Secured Areas. The walls, floors, ceilings, windows and lockable doors shall be approved by the Security Authority and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

PHYSICAL PROTECTIVE MEASURES FOR HANDLING AND STORING EUCI

130. EUCI which is classified RESTREINT UE/EU RESTRICTED may be handled:

a) in a Secured Area;

b) in an Administrative Area provided the EUCI is protected from access by unauthorised persons; or

c) outside a Secured Area or an Administrative Area provided the holder carries the EUCI in accordance with Part II, Section III, paragraphs 86-88, 90, 92, 95 and 97 of these Security Rules and has undertaken to comply with compensatory measures laid down in security instructions issued by the Head of Security Unit to ensure that EUCI is protected from access by unauthorised persons.

131. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with compensatory measures laid down in security instructions issued by the Head of Security Unit.

132. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:

a) in a Secured Area;

b) in an Administrative Area provided the EUCI is protected from access by unauthorised persons; or

c) outside a Secured Area or an Administrative Area provided the holder:

i. carries the EUCI in accordance with Part II, Section III, paragraphs 86-100 of these Security Rules;

ii. has undertaken to comply with compensatory measures laid down in security instructions issued by the Head of Security Unit to ensure that EUCI is protected from access by unauthorised persons;

iii. keeps the EUCI at all times under his/her personal control; and

iv. in the case of documents in paper form, has notified the relevant registry of the fact.

133. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be stored in a Secured Area either in a security container or in a strong room.

134. EUCI which is classified TRÈS SECRET UE/EU TOP SECRET shall be handled in a Secured Area.

135. EUCI which is classified TRÈS SECRET UE/EU TOP SECRET shall be stored in a Secured Area under one of the following conditions:

a) in a security container in line with paragraph 113 with at least one of the following supplementary controls:

i. continuous protection or verification by cleared security staff or duty personnel;

ii. an approved IDS in combination with response security personnel;

b) in an IDS-equipped strong room in combination with response security personnel.

136. Rules governing the carriage of EUCI outside physically protected areas are set out in Part II, Section III of these Security Rules.

CONTROL OF KEYS AND COMBINATIONS USED FOR PROTECTING EUCI

137. The Head of Security Unit shall define procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers. Such procedures shall protect against unauthorised access.

138. Combination settings shall be committed to memory by the smallest possible number of post-holders needing to know them. Combination settings for security containers and strong rooms storing EUCI shall be changed:

a) on receipt of a new container;

b) whenever there is a change in post-holders knowing the combination;

c) whenever a compromise has occurred or is suspected;

d) when a lock has undergone maintenance or repair; and

e) at least every 12 months.

SECTION V: CLASSIFIED MEETINGS

GENERAL

Meeting preparation

139. Meetings where EUCI is planned to be discussed shall only be held in a meeting room that has been certified at the appropriated classification level or higher.

140. As a general rule, agendas should not be classified. If the agenda of a meeting mentions classified documents, the agenda itself shall not be automatically classified. Agenda items shall be worded in a way that avoids jeopardising the protection of the Union or one or more of the Member States' interests.

141. Meeting organisers shall prepare a complete list of participants prior to the meeting. Only persons with the need-to-know, who are, where appropriate security cleared to the appropriate level, and authorised where applicable, may participate in classified meetings. The invitation itself shall forewarn the participants that the meeting will discuss classified topics, at which classification level and that corresponding security measures will apply.

142. Meeting organisers shall inform in advance the EPPO Security Unit in case of any classified meetings organised by EPPO to allow timely support for the organisation of the meeting. Equally, the meeting organisers shall inform the EPPO Security Unit of any external visitors who will attend a classified meeting organised by EPPO. Participants will be required to prove they hold a valid Personnel Security Clearance at the appropriate level in order to be able to attend the meeting. A PSCC or other proof of security assurance shall be forwarded by the NSA or other competent authority to the EPPO Security Unit, or exceptionally be presented by the delegate concerned

143. If a classified meeting requires the use of IT equipment, only accredited CIS shall be used and security measures required for the protection of EUCI handled in CIS shall be implemented.

144. Participants shall be reminded that unauthorised portable electronic devices are to be left outside the meeting room where the classified meeting is held.

Procedures to be followed during the meeting

145. At the start of the classified discussion, the Chair shall announce to the meeting participants that it is moving into classified mode. The doors shall be closed.

146. Only the necessary number of documents shall be signed for and issued to participants and interpreters, as appropriate, at the start of the meeting.

147. EUCI documents shall not be left unattended during any breaks in the classified meeting.

148. At the end of the meeting, the participants and interpreters shall be reminded not to leave any EUCI documents or notes. Any EUCI documents not required by the participants at the end of the meeting, and in any case all interpreter's documents, shall be signed for and returned to the Registry Officers.

SECURITY MEASURES TO BE APPLIED AT THE TIME OF SPECIFIC MEETINGS HELD OUTSIDE THE EPPO PREMISES AND INVOLVING EUCI

General

149. As a general rule, the EPPO shall hold meetings involving EUCI at EPPO premises (see section V). When meetings are held outside the EPPO premises, at premises where security measures equivalent or more stringent to these Security Rules are not applied, and where justified by the particular security requirements relating to the classification of the information dealt with, security measures shall be taken as described below.

Responsibilities

150. The EPPO Security Unit shall co-operate with the competent authorities of the host Member State on whose territory the meeting is being held in order to ensure the security of the meeting and the security of the delegates and their staff.

151. As regards the protection of security, the EPPO Security Unit shall specifically ensure that:

a) plans are drawn up to deal with security threats and security-related incidents whereby the measures in question cover in particular the safe custody of EUCI; and

b) if necessary, measures are taken to provide possible access to the EPPO CIS for the receipt and transmission of EUCI. The host Member State will be requested to provide access, if required, to secure communication channels.

152. A meeting security officer shall be designated from the EPPO Security Unit and be responsible for the general preparation and control of general internal security measures and for co-ordination with the other security authorities concerned. The measures taken by him or her shall in general relate to:

a) protective measures at the meeting place to ensure that the meeting is conducted without any incident that might compromise the security of any EUCI that may be used there;

b) checking personnel who have access to the place of the meeting, to delegations' areas and to conference rooms, and checking any equipment;

c) constant co-ordination with the competent authorities of the host Member State and with the Security Services; and

d) the inclusion of security instructions in the meeting dossier with due regard for the requirements set out in these security rules and any other security instructions considered necessary.

Security measures

153. The following security areas shall be established where CONFIDENTIEL UE/EU CONFIDENTIAL or above will be handled:

a) a Secured Area, consisting of the conference room and interpreters' and sound engineers' booths;

b) a Secured Area consisting of a drafting room, the security offices and reprographic equipment, as well as delegations' offices as appropriate; and

c) Administrative Areas, consisting of the Press Centre and those parts of the meeting place that are used for administration, catering and accommodation, as well as the area immediately adjacent to the Press Centre and the meeting place.

154. Administrative Areas shall be established for all meeting rooms, offices and other areas where RESTREINT UE/EU RESTRICTED will be handled.

155. The meeting security officer shall issue appropriate badges as requested by the delegations according to their needs. Where required, a distinction may be made regarding access to different security areas.

156. The security instructions for the meeting shall require all persons concerned to wear and display their badges prominently at all times within the place of the meeting, so that they can be checked as needed by security personnel.

157. Apart from badge-holding participants, admission to the meeting place shall be limited as required by these Security Rules.

158. Prior to the meeting, a special assessment shall be carried out to determine what types of equipment the meeting participants and visitors will be allowed to bring into which areas. The assessment shall, amongst others, take into account the level of EUCI that will be processed and the threat level to the information.

159. Pass-holders allowed access to an Administrative Areas may normally, without a prior check, bring in their briefcases and portable computers, equipped with their own power supply. The meeting security officer shall assess if more stringent measures for the inspection of briefcases and portable computers need to be laid down, especially to protect EUCI in Secured Areas.

160. The meeting room may be established as a technically Secured Area in accordance with these Security Rules. In such situations, it shall be made technically secure by a technical security team, which may also conduct electronic surveillance during the meeting.

161. Participants shall be responsible for taking EUCI to and from meetings. They shall also be responsible for the verification and security of those documents during their use in the meeting. Assistance from the host Member State may be requested for the transportation of classified documents to and from the place of the meeting.

162. If the EPPO Security Unit or participants are unable to store their classified documents in accordance with approved standards, they may lodge those documents in a sealed envelope with the meeting security officer, against receipt, allowing the latter to store the documents in accordance with approved standards.

163. All waste shall be treated as EUCI, and waste-paper baskets or bags shall be given to the meeting security officer, who will arrange for its destruction according to these Security Rules.

164. At the end of the meeting, all documents held, but no longer needed, shall be treated as waste by the participants. A thorough search of the meeting premises shall be made by the EPPO Security Unit before the security measures adopted for the meeting are lifted.

Documents for which a receipt was signed shall, as far as applicable, be destroyed as prescribed in these Security Rules.

SECTION VI: BREACHES OF SECURITY AND COMPROMISE OF EUCI

165. All post-holders who handle EUCI shall be thoroughly briefed on their responsibilities in this domain. They shall report immediately to the EPPO Security Unit any breach of these security rules which may come to their notice.

166. When the EPPO Security Unit is informed of or there are reasonable grounds to assume breach of security relating to EUCI or the loss or disappearance of EUCI, it shall take timely action in order to:

a) establish the facts;

b) ensure that the case is investigated by post-holders not immediately concerned with the breach;

c) assess and minimise the damage;

d) prevent a recurrence;

e) inform the EPPO Security Authority;

f) notify the Data Protection Officer when personal data may be affected; and

Exceptions to these steps shall be considered if they are likely to jeopardise the investigation.

167. Within the notifications in accordance with points 159(e - f), the following information shall be provided:

a) a description of the information involved, including its classification and where relevant its reference and copy number, date, originator, subject and scope;

b) a brief description of the circumstances of the breach of security, including the date and the period during which the information was exposed to compromise; and

c) a statement of whether the originator has been informed.

168. When informed that a breach of security has occurred, the Security Authority shall:

a) inform the originator;

b) notify the appropriate authorities of actions taken;

c) inform any European Prosecutor concerned and the College accordingly;

d) ensure that the EPPO Security Unit carries out a further investigation;

e) obtain a report from the EPPO Security Unit on the circumstances of the breach, the date or period during which it may have occurred and was discovered, including a detailed description of the content and classification of the material involved. Damage to the interests of EPPO, the Union or to one or more of its Member States and action taken to prevent a recurrence shall also be included in this report.

169. Any EPPO post-holder that is responsible for compromising EUCI or for a security breach of the security provisions laid down in these Security Rules shall be liable to disciplinary action according to the relevant rules and regulations. Such action shall be without prejudice to any other legal action.

170. This paragraph is without prejudice to the rules on the processing of personal data and the related provisions concerning the identification of a breach of personal data.

SECTION VII: PROTECTION OF EUCI HANDLED IN CIS

INTRODUCTION

171. This Section sets out provisions for implementing the provisions in Part I of these Security Rules regarding the protection of EUCI handled in CIS.

THE ACCREDITATION PROCESS

172. The accreditation process of CIS that handle EUCI at EPPO shall be aligned with the relevant security guidelines developed by the Security Committee of the Council in accordance with Article 6(2) of Council Decision 2013/488/EU on the security rules for protecting EU classified information and College Decision 014/2024 on Security Rules applicable to the Digital Communication and Information Systems of the EPPO.

173. The accreditation process of a CIS handling EUCI shall consist of the following steps:

a) The establishment of a Project for the establishment of the accredited CIS;

b) System Specific Risk Assessment (SSRA) carried out as part of the Project based on the business needs, technical implementation and accreditation scope identified by the Business Owner;

d) Approval of the SSRA by the Security Accreditation Authority based on the recommendation of the Head of Security Unit;

e) Implementation of the CIS and the security requirements defined in the SSRA by the ICT Project;

f) If deemed necessary in the SSRA, external evaluation of the security implementation of the CIS;

g) Approval of the CIS implementation, including the residual risk, and draft accreditation documentation, prepared by the ICT Project, by the Security Authority;

h) Accreditation of the CIS implementation by the Security Accreditation Authority.

174. All CIS shall, no less than once a year, undergo routine control procedures by the Digital Services Unit to ensure that all security features of the system are still valid.

175. For any given CIS, the accreditation process must be re-iterated at intervals defined during the accreditation process. The re-iteration period for the accreditation of CIS must not exceed three years.

176. After any modification, repair or failure which could have affected the security features of the system, the Head of Security Unit shall verify that a check is made to ensure the correct operation of the security features. The findings shall be reported by the Head of Security Unit to the Security Authority. Continued accreditation of the system shall depend on the satisfactory completion of the checks

INFORMATION ASSURANCE PRINCIPLES

177. The provisions set out below shall form the principles for the security of any CIS handling EUCI. The EPPO shall follow the requirements for implementing these provisions, where appropriate, as defined through IA security policies and security guidelines adopted, respectively, by the Council and the Council Security Committee.

Security risk management

178. Security risk management shall be an integral part of defining, developing, operating and maintaining CIS at EPPO.

179. Risk management (assessment, treatment, acceptance and communication) shall be conducted as an iterative process by the implementing project, using a proven, transparent and fully understandable risk assessment process. The scope of the CIS and its assets shall be clearly defined at the outset of the risk management process.

180. The Head of Security Unit 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.

181. Identified security risks shall be addressed (treated) by applying a set of security measures which results in a satisfactory balance between user requirements, cost and residual security risk.

182. The specific requirements, scale and the degree of detail, shall be commensurate with the assessed risk, taking account of all relevant factors, including the classification level of the EUCI handled in the CIS.

Security throughout the CIS life-cycle

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

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

185. Any CIS at EPPO handling EUCI, 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 they are correctly implemented, integrated and configured.

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

187. Security documentation for a CIS shall evolve over its life-cycle as an integral part of the process of change and configuration management.

Best practice and lessons learned

188. The protection of EUCI handled on CIS shall draw on best practices and lessons learned by entities involved in IA within and outside the Union.

Defence in depth

189. To mitigate risk to CIS, a range of technical and non-technical security measures, organised as multiple layers of defence, shall be implemented. These 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.

Principle of minimality and least privilege

190. Only the essential functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risk.

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

192. Systems shall be specified and designed in a way that facilitates the allocation of duties and responsibilities to post-holders so as to prevent one person having full knowledge or control of the security system's key points. The aim shall be that collusion between two or more persons would be necessary for alteration or intentional degradation of the system or network to take place.

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

Information Assurance awareness

194. Information assurance awareness training, regarding the processing of EUCI in CIS, shall be developed. The training shall ensure that the participants understand:

a) that security failures may significantly harm the CIS;

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.

195. To ensure that security responsibilities are understood, IA education and awareness training shall be mandatory for all personnel involved in the life-cycle of CIS, including senior management and CIS users.

Evaluation and approval of IT-security products

196. The required 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 security guidelines.

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

Transmission within Secured and Administrative Areas

198. Notwithstanding the provisions of this Decision, when transmission of EUCI is confined within Secured Areas or Administrative Areas, unencrypted transmission 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.

Secure interconnection of CIS

199. A CIS shall treat any interconnected IT system as untrusted and shall implement protective measures to control the exchange of classified information.

200. 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 College;

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

c) Boundary Protection Services (BPS) shall be implemented at the perimeter of all CIS.

201. There shall be no interconnection between an accredited CIS and an unprotected or public network, except where the CIS has approved BPS installed for such a purpose between the CIS and the unprotected or public network. The security measures for such interconnections shall be reviewed by Head of Security Unit and approved by the SAA.

202. When the unprotected or public network is used solely as a carrier and the data is encrypted by a cryptographic product approved in accordance with these Security Rules, such a connection shall not be deemed to be an interconnection.

203. The direct or cascaded interconnection of a CIS accredited to handle TRÈS SECRET UE/EU TOP SECRET to an unprotected or public network shall be prohibited.

Computer storage media

204. Users shall take the responsibility for ensuring that EUCI is stored on media protected in accordance with these Security Rules. Procedures shall be established to ensure that, for all levels of EUCI, the storage of information on computer storage media is being carried out in accordance with these Security Rules.

205. Computer storage media used for the storage of EUCI shall be destroyed in accordance with an approved procedure.

206. Computer storage media shall be reused, downgraded or declassified in accordance with security guidelines established by the Council.

Control and accountability of information

207. Automatic audit trails or manual logs shall be kept as a record of access to information classified SECRET UE/EU SECRET and above. These records shall be retained in accordance with these Security Rules.

INFORMATION ASSURANCE FUNCTIONS AND AUTHORITIES

208. The following IA functions shall be established at EPPO.

Information Assurance Authority

209. The Information Assurance Authority (IAA) shall be responsible for:

a) developing IA security policies and security guidelines and monitoring their effectiveness and pertinence;

b) safeguarding and administering technical information related to cryptographic products;

c) ensuring that IA measures selected for protecting EUCI comply with the relevant policies governing their eligibility and selection;

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

e) coordinating training and awareness on IA; and

f) consulting with the system provider, the security actors and representatives of users in respect to IA security policies and security guidelines;

g) monitoring implementation and application of the SecOps and, where appropriate, delegating operational security responsibilities to the system owner;

h) conducting security analysis reviews and tests, in particular to produce the relevant risk reports, as required by the SAA.

TEMPEST Authority

210. The TEMPEST Authority shall be responsible for ensuring compliance of CIS with TEMPEST policies and guidelines. To this end, the TEMPEST Authority shall approve TEMPEST countermeasures for installations and products to protect EUCI to a defined level of classification in its operational environment.

Crypto Distribution Authority

211. As the Crypto Distribution Authority , the Head of Security Unit shall be responsible for:

a) managing and handling all cryptographic materials and products, ensuring the custody of crypto and controlled items and, if so required, ensuring the generation of cryptographic variables;

b) ensuring that appropriate procedures are enforced and channels established for accounting, secure handling, storage and distribution of all EU crypto material; and

c) ensuring the transfer of EU crypto material to or from persons or services using it.

Security Accreditation Authority

212. The Security Accreditation Authority (SAA)shall be responsible for:

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

b) establishing a security accreditation process, in accordance with the relevant policies, clearly stating the approval conditions for CIS under its authority;

c) defining a security accreditation strategy setting out the degree of detail for the accreditation process commensurate with the required level of assurance;

d) examining and approving security-related documentation, including risk management and residual risk statements, security implementation verification documentation and security operating procedures ("SecOPs"), and ensuring that it complies with the EPPO's security rules and policies;

e) approving implementation of security measures in relation to the CIS by undertaking or sponsoring security assessments, inspections or reviews;

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

g) endorsing the selection of approved cryptographic and TEMPEST products used to provide security for a CIS;

h) approving, or where relevant, participating in the joint approval of the interconnection of a CIS to other CIS;

i) consulting, where necessary, 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; and

j) accrediting all CIS and components thereof operating within the remits of EPPO.

Information Assurance Operational Authority

213. As the IA Operational Authority (IAOA) for all CIS shall be responsible for:

a) developing security documentation in line with security policies and security guidelines, in particular the SSRA including the residual risk statement, the SecOPs and the crypto plan within the CIS accreditation process;

b) participating in selecting and testing the system-specific technical security measures, devices and software, to supervise their implementation and to ensure that they are securely installed, configured and maintained in accordance with the relevant security documentation;

c) participating in selecting TEMPEST security measures and devices if required in the SSRA and ensuring that they are securely installed and maintained in cooperation with the TA;

d) providing CIS-specific IA training; and

e) with the support of the Digital Services Unit, implementing and operating CIS-specific security measures.

SECTION VIII: INDUSTRIAL SECURITY

INTRODUCTION

214. This Section lays down general security provisions applicable to private parties in pre-contract negotiations and throughout the life-cycle of classified contracts let by the EPPO.

215. Such contracts shall not involve information classified TRES SECRET UE- EU TOP SECRET

216. The EPPO shall, where relevant, apply and follow guidelines on industrial security established by the Council or the Security Committee of the Council.

SECURITY ELEMENTS IN A CLASSIFIED CONTRACT

Security classification guide (DSA)

217. Prior to launching a call for tender or letting a classified contract, EPPO, 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, the EPPO shall prepare an SCG to be used for the performance of the contract.

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

a) in preparing an SCG, the EPPO Security Unit shall perform a risk assessment taking into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;

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

c) where relevant, the EPPO Security Unit shall liaise with the Member States' NSAs/DSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the SCG.

Security aspects letter (SAL)

219. The contract-specific security requirements, identified in the risk assessment, shall be described in a SAL. The SAL shall, where appropriate, contain the SCG and shall be an integral part of a classified contract or sub-contract.

220. The SAL shall contain the provisions requiring the contractor and/or subcontractor to comply with the minimum standards laid down in these Security Rules. Non-compliance with these minimum standards may constitute sufficient grounds for the contract to be terminated.

Programme/Project Security Instructions (PSI)

221. Depending on the scope of programmes or projects involving access to, handling or storage of EUCI, specific PSI may be prepared by the EPPO designated to manage the programme or project. The PSI shall require the approval of the Member States' NSAs/DSAs or any other competent security authority participating in the PSI and may contain additional security requirements.

FACILITY SECURITY CLEARANCE (FSC)

222. Where relevant, the EPPO, as the contracting authority, shall notify the appropriate NSA/DSA or any other competent security authority that an FSC is required in the pre-contractual stage or for performing the contract. An FSC or PSC shall be required in the pre-contractual stage where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the bidding process.

223. The EPPO shall not award a classified contract to a preferred bidder before having received confirmation from the NSA/DSA or any 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.

224. In the case of a sub-contract, the NSA/DSA or any other competent security authority shall be informed accordingly.

225. Withdrawal of an FSC by the relevant NSA/DSA or any other competent security authority shall constitute sufficient grounds for the EPPO, as the contracting authority, to terminate a classified contract or exclude a bidder from the competition.

CLASSIFIED CONTRACTS AND SUB-CONTRACTS

226. Where EUCI is provided to a bidder at the pre-contractual stage, the invitation to bid shall contain a provision obliging the bidder which fails to submit a bid or which is not selected to return all classified documents within a specified period of time.

227. Once a classified contract or sub-contract has been awarded, the EPPO, as the contracting authority, shall notify the contractor's or subcontractor's NSA/DSA or any other competent security authority about the security provisions of the classified contract.

228. When such contracts are terminated, the EPPO, as the contracting authority (and/or the NSA/DSA or any other competent security authority, as appropriate, in the case of a sub-contract) shall promptly notify the NSA/DSA or any other competent security authority of the Member State in which the contractor or subcontractor is registered.

229. As a general rule, the contractor or subcontractor shall be required to return to the contracting authority, upon termination of the classified contract or sub-contract, any EUCI held by it.

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

231. Where the contractor or subcontractor is authorised to retain EUCI after termination of a contract, the minimum standards contained in these Security Rules shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor or subcontractor.

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

233. A contractor shall obtain permission from the EPPO, as the contracting authority, before sub-contracting any parts of a classified contract. No subcontract may be awarded private parties registered in a non-EU Member State which has not concluded a security of information Agreement with the Union.

234. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in these Security Rules and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.

235. With regard to EUCI created or handled by the contractor or subcontractor, the EPPO shall be treated by the contractor as the originator.

VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

236. Where EPPO, contractors' or subcontractors' personnel requires access to information classified 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/DSAs or any other competent security authority concerned. However, in the context of specific projects, the NSAs/DSAs may also agree on a procedure whereby such visits can be arranged directly.

237 All visitors shall hold an appropriate PSC and have a 'need-to-know' for access to the EUCI related to the EPPO contract.

238. Visitors shall be given access only to EUCI related to the purpose of the visit.

TRANSMISSION AND CARRIAGE OF EUCI

239. With regard to the transmission of EUCI by electronic means, the relevant provisions of these Security Rules shall apply.

240. With regard to the carriage of EUCI, the relevant provisions of the management of EUCI in these Security Rules shall apply, in accordance with national laws and regulations.

241. 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 these Security Rules and Annex I of Council Decision 2013/488/EU on the security rules for protecting EU classified information;

d) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan shall be drawn up by the consignor and approved by the NSA/DSAs or any other competent security authority concerned;

e) journeys shall be point to point to the extent possible, and shall be completed as quickly as circumstances permit; and

f) whenever possible, routes should be only through Member States. Routes through states other than Member States should only be undertaken when authorised by the NSA/DSA or any other competent security authority of the states of both the consignor and the consignee.

TRANSFER OF EUCI TO CONTRACTORS LOCATED IN THIRD STATES

242. EUCI shall be transferred to contractors and subcontractors located in third states in accordance with security measures agreed between the EPPO, as the contracting authority, and the NSA/DSA of the concerned third state where the contractor is registered.

INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

243. In liaison, as appropriate, with the NSA/DSA of the Member State, the EPPO, as the contracting authority, shall be entitled to conduct inspections of the 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.

244. To the extent necessary under national laws and regulations, NSAs/DSAs or any other competent security authority shall be notified by the EPPO as the contracting authority of contracts or subcontracts containing information classified RESTREINT UE/EU RESTRICTED.

245. An FSC or a PSC for contractors or subcontractors and their personnel shall not be required for contracts let by the EPPO containing information classified RESTREINT UE/EU RESTRICTED.

246. The EPPO, as the contracting authority, shall examine the responses to invitations to tender for contracts which require access to information classified RESTREINT UE/EU RESTRICTED, notwithstanding any requirement relating to FSC or PSC which may exist under national laws and regulations.

247. The conditions under which the contractor may subcontract shall be in accordance with paragraph 232.

248. Where a contract involves handling information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor, the EPPO as contracting authority shall ensure that the contract or any subcontract specifies the necessary technical and administrative requirements regarding accreditation of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation of such CIS shall be agreed between the contracting authority and the relevant NSA/DSA.

APPENDIX 1: EQUIVALENCE OF SECURITY CLASSIFICATIONS

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota (1) below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czechia	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Germany	STRENG GEHEIM	GEHEIM	VS (2) – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
France	TRÈS SECRET TRÈS SECRET DÉFENSE (3)	SECRET SECRET DÉFENSE (3)	CONFIDENTIEL DÉFENSE (3), (4)	nota (5) below
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo

Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted (6)
Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden	Kvalificerat hemlig	Hemlig	Konfidentiell	Begränsat hemlig

(1) 'Diffusion Restreinte/Beperkte Verspreiding' is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

(2) Germany: VS = Verschlusssache.

(3) Information generated by France before 1 July 2021 and classified 'TRÈS SECRET DÉFENSE', 'SECRET DÉFENSE' or 'CONFIDENTIEL DÉFENSE' continues to be handled and protected at the equivalent level of 'TRÈS SECRET UE/EU TOP SECRET', 'SECRET UE/EU SECRET' or 'CONFIDENTIEL UE/EU CONFIDENTIAL' respectively.

(4) France handles and protects 'CONFIDENTIEL UE/EU CONFIDENTIAL' information in accordance with the French security measures for protecting 'SECRET' information.

(5) France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

(6) The Maltese and English markings for Malta can be used interchangeably.