

# Official Journal of the European Union

L 311



English edition

Legislation

Volume 62

2 December 2019

Contents

## II *Non-legislative acts*

### DECISIONS

- ★ **Commission Decision (EU, Euratom) 2019/1961 of 17 October 2019 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information** ..... 1
- ★ **Commission Decision (EU, Euratom) 2019/1962 of 17 October 2019 on implementing rules for handling RESTREINT UE/EU RESTRICTED information** ..... 21
- ★ **Commission Decision (EU, Euratom) 2019/1963 of 17 October 2019 laying down implementing rules on industrial security with regard to classified procurement contracts** ..... 37

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.



## II

*(Non-legislative acts)*

## DECISIONS

**COMMISSION DECISION (EU, Euratom) 2019/1961****of 17 October 2019****on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on security in the Commission <sup>(1)</sup>,

Having regard to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information <sup>(2)</sup>,

Having regard to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission <sup>(3)</sup>,

Whereas:

- (1) Decision (EU, Euratom) 2015/444 applies to all Commission departments and in all premises of the Commission.
- (2) Security measures for protecting EU classified information (EUCI) throughout its life-cycle are to be commensurate in particular with its security classification.
- (3) Articles 4(3), 19(1)(c) and 22 of Decision (EU, Euratom) 2015/444 provide that more detailed provisions to supplement and support implementation of the Decision are to be laid down in implementing rules, governing issues such as a classification guide, compensatory measures for handling EUCI outside a Secured Area or an Administrative Area, and originator responsibilities.
- (4) Where necessary, implementing rules to supplement or support Decision (EU, Euratom) 2015/444 are to be adopted in accordance with Article 60 of that Decision.
- (5) Security measures taken to implement this Decision are to comply with the principles for security in the Commission set out in Article 3 of Decision (EU, Euratom) 2015/443.
- (6) The Council, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy have agreed to ensure maximum consistency in the application of security rules regarding their protection of EUCI while taking into account their specific institutional and organisational needs, in accordance with the declarations attached to the minutes of the Council session at which Council Decision 2013/488/EU <sup>(4)</sup>.
- (7) On 4 May 2016 the Commission adopted a decision <sup>(5)</sup> empowering the Member of the Commission responsible for security matters to adopt, on behalf of the Commission and under its responsibility, the implementing rules provided for in Article 60 of Decision (EU, Euratom) 2015/444,

<sup>(1)</sup> OJ L 72, 17.3.2015, p. 41.

<sup>(2)</sup> OJ L 72, 17.3.2015, p. 53.

<sup>(3)</sup> OJ L 6, 11.1.2017, p. 40.

<sup>(4)</sup> Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

<sup>(5)</sup> Commission Decision of 4 May 2016 on an empowerment relating to security, C(2016) 2797 final.

HAS ADOPTED THIS DECISION:

## CHAPTER 1

### GENERAL PROVISIONS

#### Article 1

#### **Subject matter and scope**

1. This Decision sets out the handling conditions for EU classified information (EUCI) of CONFIDENTIEL UE/EU CONFIDENTIAL <sup>(6)</sup> and SECRET UE/EU SECRET <sup>(7)</sup> level in compliance with Decision (EU, Euratom) 2015/444.
2. This Decision shall apply to all Commission departments and in all premises of the Commission.

#### Article 2

#### **Criteria for access to CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information**

1. Access to information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be granted after:
  - (a) The need for an individual to have access to certain CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information in order to be able to perform a professional function or task for the European Commission has been determined;
  - (b) The individual has been briefed on the rules and the relevant security standards and guidelines for protecting CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information;
  - (c) The individual has acknowledged their responsibilities for protecting the information concerned; and
  - (d) The individual has been authorised by the Commission security authority to access EUCI up to the relevant level and until a specified date in accordance with Article 10(1)3 of Decision (EU, Euratom) 2015/444.
2. Commission trainees shall not be given duties that require them to have access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.
3. Access shall be withheld or permitted for other categories of staff in accordance with the table set out in the Annex.

## CHAPTER 2

### CREATING CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION

#### Article 3

#### **Originator**

While the originator within the meaning of Article 1 of Decision (EU, Euratom) 2015/444 is the Union institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the Union's structures, the drafter of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information will not necessarily be the same.

<sup>(6)</sup> Pursuant to Article 3 of Decision (EU, Euratom) 2015/444, CONFIDENTIEL UE/EU CONFIDENTIAL information shall mean 'information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States'.

<sup>(7)</sup> Pursuant to Article 3 of Decision (EU, Euratom) 2015/444, SECRET UE/EU SECRET information shall mean 'information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States'.

*Article 4***Assigning a classification level**

1. Staff drafting a document on the basis of information within the meaning of Article 1 shall always consider whether their document needs to be classified. Classifying a document as EUCI shall involve an assessment and a decision by the originator as to whether the disclosure of the document to unauthorised persons would cause prejudice to the interests of the European Union or of one or more of the Member States. If drafters are in any doubt as to whether the document they are drafting warrants being classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET they should consult the Head of Unit or Director responsible.

2. A document shall be classified as at least CONFIDENTIEL UE/EU CONFIDENTIAL if its unauthorised disclosure could, inter alia:

- (a) materially damage diplomatic relations, i.e. cause formal protest or other sanctions;
- (b) prejudice individual security or liberty;
- (c) cause damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the effectiveness of valuable security or intelligence operations;
- (d) substantially undermine the financial viability of major organisations;
- (e) impede the investigation of or facilitate serious crime;
- (f) work substantially against the Union's or Member States' financial, monetary, economic and commercial interests;
- (g) seriously impede the development or operation of major Union policies;
- (h) shut down or otherwise substantially disrupt significant Union activities;
- (i) lead to the discovery of information classified at a higher level.

3. Information shall be classified as at least SECRET UE/EU SECRET if its unauthorised disclosure could, inter alia:

- (a) raise international tensions;
- (b) seriously damage relations with third countries or international organisations;
- (c) threaten life directly or seriously prejudice public order or individual security or liberty;
- (d) cause serious damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the continuing effectiveness of highly valuable security or intelligence operations;
- (e) cause substantial material damage to the Union's or Member States' financial, monetary, economic or commercial interests;
- (f) lead to the discovery of information classified at a higher level.

4. Originators may decide to attribute a standard classification level to categories of information that they create on a regular basis. However, they shall ensure that individual pieces of information are given the appropriate classification level.

*Article 5***Working with drafts**

1. Information shall be classified as soon as it is produced. Personal notes, preliminary drafts or messages containing information that warrants classification at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be marked as such from the outset and shall be produced and handled in accordance with this Decision.
2. If the final document no longer warrants the initial classification level it shall be downgraded or declassified.

*Article 6***Record of source material**

In order to enable the exercise of originator control in accordance with Article 14, originators of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall keep a record of any classified sources used for producing classified documents, including details of sources originally from EU Member States, international organisations or third countries. Where appropriate, aggregated classified information shall be marked in such a way as to preserve the identification of the originators of the classified source materials used.

*Article 7***Classifying parts of a document**

1. In accordance with Article 22(6) of Decision (EU, Euratom) 2015/444, the overall classification level of a document shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final aggregated document shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.
2. Documents containing classified and non-classified parts shall be structured and marked so that components with different classification and/or sensitivity levels can be easily identified and detached if necessary. This shall enable each part to be handled appropriately when detached from the other components.

*Article 8***Full classification marking**

1. Information that warrants classification shall be marked and handled as such regardless of its physical form. The classification level shall be clearly communicated to recipients, either by a classification marking, if the information is delivered in written form, whether this is on paper, on removable storage media or in a Communication and Information System (CIS), or by an announcement, if the information is delivered in oral form, such as in a conversation or a presentation. Classified material shall be physically marked so as to allow for easy identification of its security classification.
2. On documents, the full classification marking CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be written in block capitals, in full in French and English (French first), in accordance with paragraph 3. The marking shall not be translated into other languages.
3. The CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET classification marking shall be affixed as follows:
  - (a) centred at the top and bottom of every page of the document;
  - (b) the complete classification marking on one line, with no spaces either side of the forward slash;
  - (c) in capitals, black, font Times New Roman 16 (when possible, but at least 14), bold and surrounded by a border on each side.

4. When creating a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET 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, a registration number and a subject, which itself shall not be classified information unless it is marked as such;
  - (d) all the annexes and enclosures shall be listed, whenever possible on the first page; and
  - (e) the document shall have the date of its creation on it.
5. When possible, the SECRET UE/EU SECRET marking shall appear in red.

#### Article 9

##### Abbreviated C-UE/EU-C and S-UE/EU-S classification markings

The abbreviations C-UE/EU-C and S-UE/EU-S may be used to indicate the classification level of individual parts respectively of a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET document or where the full classification marking cannot be inserted, for example on a small removable storage medium. It may be used in the body of text where repeated use of the full classification markings is cumbersome. The abbreviation shall not be used instead of the full classification markings in the header and footer of the document.

#### Article 10

##### Other security designators

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents may bear other markings, or 'security designators', specifying, for example, the field to which the document relates, or indicating a particular distribution on a need-to-know basis. An example is:

|                                    |
|------------------------------------|
| <b>RELEASABLE TO LIECHTENSTEIN</b> |
|------------------------------------|

2. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents may bear a security caveat that gives specific instructions on how to handle and manage the documents.
3. Whenever possible, any indications for downgrading or declassifying shall be affixed on the first page of the document at the time it is created. For example, the following marking may be used:

|                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p style="text-align: center;"><b>SECRET UE/EU SECRET</b><br/>until [dd.mm.yyyy]<br/><br/>and <b>RESTREINT UE/EU RESTRICTED</b><br/><br/>thereafter</p> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Article 11

##### Electronic processing

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall be created using electronic means, where these are available.
2. When creating CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information, Commission staff shall use CIS accredited for the corresponding classification level or for a higher classification level. Staff shall consult their Local Security Officer (LSO) if there is any doubt as to which CIS may be used. In consultation with the Commission security authority specific procedures may be applied in emergencies or in specific technical configurations.

3. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents, including drafts, as required by Article 5, shall not be sent by email, printed or scanned on standard printers or scanners, or handled on the personal devices of members of staff. Only printers or copiers connected to standalone computers protected from electromagnetic emissions or to an accredited system shall be used to print out CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents.

#### Article 12

##### Registration for security purposes

1. Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be registered for security purposes prior to distribution and on receipt. It shall be registered:

- when it arrives in or leaves an organisational entity; and
- when it arrives in or leaves a CIS.

2. This registration may be carried out in paper or in electronic logbooks.

3. If the information is handled electronically within a CIS, these recording procedures may be performed by processes within the CIS itself. In this case, the CIS shall include measures to guarantee the integrity of the log records.

4. The Registry Control Officer shall keep a register that contains at least the following information for each document:

- (a) the date the final classified document was registered;
- (b) the classification level;
- (c) where applicable, the expiry date of the classification level;
- (d) the name of the originating department;
- (e) the recipient or recipients;
- (f) the subject;
- (g) the originating department's reference number for the document;
- (h) the registration number
- (i) the number of copies circulated;
- (j) where possible, the log of sources used for creating the document;
- (k) the date of downgrading or declassification of the document; and
- (l) destruction details (place, date, method, supervision, destruction certificate).

#### Article 13

##### Distribution

The sender of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents shall decide who to distribute the information to, based on their need-to-know. A distribution list shall be drawn up in order to further enforce the need-to-know principle.

## CHAPTER 3

**WORKING WITH EXISTING CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION***Article 14***Originator control**

1. The originator shall have 'originator control' over CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information which it has created. The originator's prior written consent shall be sought before the information can be:

- (a) declassified or downgraded;
- (b) used for purposes other than those established by the originator;
- (c) released to a third country or international organisation;
- (d) disclosed to a party outside the Commission but within the EU; or
- (e) disclosed to a contractor or prospective contractor located in a third country.

2. Holders of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information are duly authorised individuals that have been given access to the classified information in order to be able to perform their duties. They are responsible for the correct handling, storage and protection of it in accordance with Decision (EU, Euratom) 2015/444. Unlike originators of classified information, holders shall not be authorised to decide on the downgrading, declassification or onward release of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

3. If the originator of a piece of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information cannot be identified, the Commission department holding that classified information shall exercise originator control. The Commission Security Expert Group shall be consulted before CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information is released to a third country or international organisation.

*Article 15***CIS suitable for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information**

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be handled and transmitted by electronic means, where these are available. Only CIS and equipment that has been accredited by the Commission security accreditation authority for handling information classified at the relevant level or a higher classification level shall be used.

2. Where a Commission department has the appropriate equipment to handle and send information classified at these levels it shall assist other Commission entities in handling and sending information appropriately, as far as it is able to do so.

*Article 16***Specific measures for CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information on removable storage media**

1. The use of removable storage media shall be strictly controlled and accounted for. Only removable storage media provided by the Commission and encrypted by a product approved by the Commission security authority shall be used. Personal removable storage media and those given freely at conferences, seminars, etc. shall not be used for transferring classified information. Where possible, Tempest-proof removable storage media should be used, in accordance with the guidance from the Commission security authority.

2. Where a classified document is handled or stored electronically on removable storage media, such as USB sticks, CDs or memory cards, the classification marking shall be clearly visible on the displayed information itself, as well as in the filename and on the removable storage medium.
3. Staff shall bear in mind that when large amounts of classified information are stored on removable storage media the device may warrant a higher classification level.
4. Only CIS that have been appropriately accredited shall be used to transfer CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information onto or from removable storage media.
5. When downloading such information on removable storage media, particular care shall be taken to ensure that the media does not contain viruses or malware prior to the transfer of the data.
6. Where applicable, removable storage media shall be handled in accordance with any security operating procedures relating to the encryption system used.
7. Documents on removable storage media that are either no longer required, or have been transferred onto an appropriate CIS, shall be securely removed or deleted using approved products or methods. Unless stored in an appropriate safe, removable storage media shall be destroyed when no longer needed. Any destruction or deletion shall use a method that is in accordance with the Commission security rules. An inventory shall be kept of the removable media, and their destruction shall be registered.

#### Article 17

##### **Handling and storage of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information**

1. In accordance with Article 19(3)(a) of Decision (EU, Euratom) 2015/444, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be handled in a Secured Area <sup>(8)</sup>.
2. Pursuant to Article 19(3)(b) of Decision (EU, Euratom) 2015/444, this information may be handled in an Administrative Area <sup>(9)</sup>, provided the EUCI is protected from access by unauthorised persons.
3. This information may be handled outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with compensatory measures as required under Article 19(3)(c) of Decision (EU, Euratom) 2015/444, which shall include at least the following:
  - CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall not be read in public places.
  - The EUCI shall be kept at all times under the personal control of the holder.
  - In the case of documents in paper form, the holder has notified the relevant registry of the fact that the classified documents are being handled outside a Secured Area and Administrative Area.
  - The documents shall be stowed in an appropriate safe when they are not being read or discussed.
  - The doors to the room shall be closed while the document is being read or discussed.
  - The details of the document shall not be discussed over the phone on a non-secured line or in an email.
  - The document shall not be photocopied or scanned by the holder. Only the registry may provide any further copies.
  - The document shall only be handled and temporarily held outside an Administrative or Secured Area for the minimum time necessary, after which it shall be returned to the registry.

<sup>(8)</sup> As defined in Article 18 of Decision (EU, Euratom) 2015/444.

<sup>(9)</sup> As defined in Article 18 of Decision (EU, Euratom) 2015/444.

- Return of the document shall be signed for.
  - The holder shall not throw the classified document away or destroy it.
4. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be stored in a Secured Area in a security container or a strong room.
  5. Further advice can be sought from the Local Security Officer (LSO) of the relevant Commission department.
  6. Any suspected or actual security incidents involving the document shall be reported to the LSO as soon as possible.

#### Article 18

##### **Copying and translating CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information**

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be copied or translated on instruction from the holder, provided the originator has not imposed any caveats. However, no more copies shall be made than are strictly necessary.
2. Where only part of a classified document is reproduced, the same conditions shall apply as for copying the full document. Extracts shall also be classified at the same level, unless the originator has specifically classified them at a lower level, or marked them as unclassified.
3. The security measures applicable to the original information shall also be applied to copies and translations thereof.

#### Article 19

##### **General principles for carrying CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information**

1. Whenever possible, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information that needs to be taken outside Secured Areas or Administrative Areas shall be sent electronically by appropriately accredited means and/or protected by approved cryptographic products.
2. Depending on the means available or the particular circumstances, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be physically carried by hand in the form of paper documents or on removable storage media. The use of removable storage media to transfer CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be given preference to sending paper documents.
3. Only removable storage media encrypted by a product approved by the Commission security authority may be used. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information on removable storage media that is not protected by an encryption product that has been approved by the Commission security authority shall be handled in the same manner as paper copy.
4. A consignment may contain more than one piece of EUCI, provided the need-to-know principle is respected.
5. The packaging used shall ensure that the contents are covered from view. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be carried in two layers of opaque packaging, such as envelopes, opaque folders or a briefcase. The outer packaging shall not bear any indication of the nature or classification level of its contents. The inner layer of packaging shall be marked as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET. Both layers shall state the intended recipient's name, job title and address, as well as a return address in case delivery cannot be made.
6. Staff or couriers hand-carrying CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall be security authorised and shall be issued with a courier certificate.

7. The envelope/package shall not be opened *en route*. The security authorisation for the courier does not authorise him/her to access the content of the classified information.

8. Any security incidents involving CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information that is carried by staff or couriers shall be reported for subsequent investigation to the Security Directorate of the Directorate-General for Human Resources and Security, via the LSO of the relevant Commission department.

#### Article 20

##### **Hand carriage of removable storage media**

1. Removable storage media that are used to transport CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be accompanied by a dispatch note, detailing the removable storage media containing the classified information, as well as all files contained on them, to allow the recipient to make the necessary verifications and to confirm receipt.

2. Only the documents to be provided shall be stored on the media. All the classified information on a single USB stick, for instance, would have to be intended for the same recipient. The sender shall bear in mind that large amounts of classified information stored on such devices may warrant a higher classification level for the device as a whole.

3. Only removable storage media bearing the appropriate classification marking shall be used to carry CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

4. Any CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information saved on removable storage media shall be registered for security purposes.

#### Article 21

##### **Carriage of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents within Commission buildings**

1. Security authorised staff may carry CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents within a Commission building, but the documents shall not leave the possession of the bearer or be read in public.

2. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall not be sent through internal mail.

#### Article 22

##### **Carriage of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents within the Union**

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be carried by staff or Commission couriers anywhere within the Union provided they comply with the following instructions:

(a) opaque double envelopes or packaging shall be used to convey CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information. The outside shall not bear any indication of the nature or classification level of its contents;

(b) the CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall not leave the possession of the bearer; and

(c) the envelope or package shall not be opened *en route* and the information shall not be read in public places.

2. Registry staff wishing to send CONFIDENTIEL UE/EU CONFIDENTIAL information to other locations in the Union may arrange for it to be conveyed by one of the following means:

- by national postal services that track the consignment or certain commercial courier services that guarantee personal hand carriage, provided that they meet the requirements set out in Article 24 of this Decision;
- by military, government or diplomatic courier.

3. Staff wishing to send SECRET UE/EU SECRET information to other Member States in the EU may only arrange with their Registry for it to be conveyed by military, government or diplomatic courier, but not by postal services or commercial couriers.

4. Commission staff or official Commission couriers bearing CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall carry a courier certificate for each consignment, issued by the respective department's registry, which certifies that the bearer is authorised to carry the consignment.

#### *Article 23*

##### **Carriage of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information from or to the territory of a third country**

1. Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be hand-carried by staff between the territory of the Union and the territory of a third country.
2. Registry staff may arrange for carriage by military or diplomatic courier.
3. When hand-carrying either paper documents or removable storage media classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, staff shall comply with all of the following additional measures:
  - When travelling by public transport the classified information shall be placed in a briefcase or bag that is kept in the bearer's personal custody. It shall not be consigned to a baggage hold.
  - The inner layer of packaging shall bear an official seal to indicate that it is an official consignment and is not to undergo security scrutiny.
  - The bearer shall carry a courier certificate, which certifies that the bearer is authorised to carry the CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignment, issued by the relevant department's registry.

#### *Article 24*

##### **Transport by commercial couriers**

1. For the purposes of this Decision, 'commercial couriers' include national postal services and commercial courier companies that offer a service where information is delivered for a fee and is either personally hand carried or tracked.
2. Commercial couriers may convey CONFIDENTIEL UE/EU CONFIDENTIAL information within a Member State or from one Member State to another Member State. Commercial couriers may convey SECRET UE/EU SECRET information only within a Member State, but not abroad.
3. Commercial courier services shall be instructed that they may deliver CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignments only to the Registry Control Officer, to his duly authorised substitute or to the intended recipient.
4. Commercial couriers may use the services of a sub-contractor. However, responsibility for complying with this Decision shall remain with the courier company.

5. Services offered by commercial couriers providing electronic transmission of registered delivery documents shall not be used for CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

#### *Article 25*

##### **Preparation of EUCI for transport by commercial courier services**

1. When classified consignments are being prepared the sender shall bear in mind that commercial courier services shall only deliver CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignments to the intended recipient, a duly authorised substitute, the registry control officer or his/her duly authorised substitute or a receptionist.
2. When such information is sent by an approved commercial courier service the consignment shall be prepared and packaged as follows:
  - (a) The consignment shall be sent using double envelopes (the inner envelope being such that any attempt to open it will be evident) or other suitably secure packing material.
  - (b) The classification level shall be clearly visible on the inner envelope or inner layer of packaging.
  - (c) The classification shall not be indicated on the outer envelope or the outer layer of packaging.
  - (d) Both the inner and outer envelopes or layers of packaging shall be clearly addressed to a named individual at the intended recipient, and shall include a return address.
  - (e) A registration receipt form shall be placed inside the inner envelope or inner layer of packaging for the recipient to complete and return. The registration receipt, which shall not itself be classified, shall quote the reference number, date and copy number of the document, but not the subject.
  - (f) Delivery receipts are required in the outer envelope or outer packaging. The delivery receipt, which itself shall not be classified, shall quote the reference number, date and copy number of the document, but not the subject.
  - (g) The courier service must obtain and provide the sender with proof of delivery of the consignment on the signature and tally record, or the courier must obtain receipts or package numbers.
3. The sender shall liaise with the named recipient before the consignment is sent to agree a suitable date and time for delivery.
4. The sender is solely responsible for any consignment sent by a commercial courier service. In the event that the consignment is lost or not delivered on time, the sender shall report it to the Commission security authority, which will follow up the security incident.

#### *Article 26*

##### **Other specific handling conditions**

1. Any carriage conditions set out in a security of information agreement or in administrative arrangements shall be complied with. If in doubt, staff shall consult their respective registry or the Security Directorate in the Directorate-General for Human Resources and Security.
2. The double packaging requirement can be waived for classified information that is protected by approved cryptographic products. However, for addressing purposes, and also as the removable storage medium bears an explicit security classification marking, the medium shall be carried in at least an ordinary envelope but may require additional physical protection measures, such as bubble wrap envelopes.

## CHAPTER 4

## CLASSIFIED MEETINGS

*Article 27***Preparing for a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting**

1. Meetings where CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information is due to be discussed shall only be held in a meeting room that has been accredited at the appropriate level or higher. Where these are not available, staff shall seek the advice of the Commission security authority.
2. As a general rule, agendas should be not classified. If the agenda of a meeting mentions classified documents, the agenda itself shall not automatically be 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.
3. Meeting organisers shall remind participants that any comments sent in on a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET agenda item must not be sent through email, or through other means that have not been appropriately accredited in accordance with Article 11 of this Decision.
4. Meeting organisers shall endeavour to group CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET items consecutively on the agenda in order to facilitate the smooth functioning of the meeting. Only persons with a need-to-know, who are security cleared to the appropriate level, and authorised where applicable, may be present during discussions of classified items.
5. The invitation itself shall forewarn the participants that the meeting will discuss classified topics, and that corresponding security measures will apply.
6. Participants shall be reminded that portable electronic devices are to be left outside the meeting room during discussion of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET items.
7. Meeting organisers shall prepare a complete list of participants prior to the meeting.

*Article 28***Participants' access to a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting**

1. Meeting organisers shall inform the Commission security authority of any external visitors who will attend a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting on Commission premises.
2. 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 discussion of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET agenda items.

*Article 29***Electronic equipment in a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting room**

1. Only accredited IT systems in accordance with Article 11 of this Decision may be used where classified information is conveyed, such as to give a presentation that displays CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information or for videoconferences.
2. The Chair shall ensure that unauthorised portable electronic devices have been left outside the meeting room.

*Article 30***Procedures to be followed during a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting**

1. At the start of the classified discussion, the Chair shall announce to the meeting that it is moving into classified mode. The doors shall be closed.
2. Only the necessary number of documents shall be signed for and issued to participants and interpreters, as appropriate, at the start of the discussion.
3. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall not be left unattended during any breaks in the meeting.
4. At the end of the meeting, the participants and interpreters shall be reminded not to leave any classified documents or classified notes they might have made lying unattended in the room. Any CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents not required by the participants at the end of the meeting, and in any case all interpreters' documents, shall be signed for and returned to the Registry Control Officer for destruction in appropriate shredders.
5. The list of participants and an outline of any classified information shared with Member States and released orally to third countries or international organisations shall be noted down during the meeting in order to be recorded in the outcome of proceedings.

*Article 31***Interpreters and translators**

Only security-cleared and authorised interpreters and translators who are subject to the Staff regulations or the Conditions of Employment of other servants of the European Union or who have a contractual link to the Commission shall have access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

## CHAPTER 5

**SHARING AND EXCHANGING CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION***Article 32***Originator consent**

If the Commission is not the originator of the classified information for which release or sharing is desired, or of the source material it may contain, the Commission department which holds this classified information shall first seek the originator's written consent to release. If the originator cannot be identified, the Commission department holding that classified information shall exercise originator control.

*Article 33***Sharing CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information with other Union entities**

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall only be shared with another Union institution, agency, body or office if the recipient has a need-to-know and the entity has a corresponding legal arrangement with the Commission.
2. Within the Commission, the EUCI Registry managed by the Secretariat-General shall as a general rule be the main point of entry and exit for classified information exchanges with other Union institutions, agencies, bodies and offices. The Commission security authority shall be consulted where there are security, organisational or operational grounds for it to be more appropriate for local EUCI registries to operate as the point of entry and exit for matters within the competence of the department concerned.

*Article 34***Exchanging CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information with Member States**

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be shared with Member States if the recipient has a need-to-know and has been security cleared.
2. Member States' classified information that bears an equivalent national classification marking <sup>(10)</sup> and which has been provided to the Commission shall be afforded the same level of protection as CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information.

*Article 35***Exchanging CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information with third countries and international organisations**

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall only be released to a third country or international organisation if the recipient has a need-to-know and the country or international organisation has an appropriate legal or administrative framework in place, such as a security of information agreement or an administrative arrangement with the Commission. The provisions of such an agreement or arrangement shall prevail over the provisions of this Decision.
2. The EUCI registry managed by the Secretariat-General shall as a general rule act as the main point of entry and exit for all information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET exchanged between the Commission and third countries and international organisations. The Commission security authority shall be consulted where there are security, organisational or operational grounds which make it more appropriate for local EUCI registries to operate as the point of entry and exit for matters within the competence of the department concerned.
3. Any classified information received from a third country or an international organisation shall be registered for security purposes. Staff shall therefore contact the registry if they receive classified information from outside the usual registry circuit.
4. To ensure traceability, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be registered:
  - when it arrives in or leaves an organisational entity; and
  - when it arrives in or leaves a CIS.
5. Such registration may be carried out on paper or in electronic logbooks.
6. Registration procedures for classified information handled within an accredited CIS may be performed by processes within the CIS itself. In that case, the CIS shall include measures to guarantee the integrity of the log records.
7. Classified information received from third countries or international organisations shall be afforded an equivalent level of protection as EUCI bearing the equivalent classification marking as set out in the respective security of information agreement or administrative arrangement.

*Article 36***Exceptional ad hoc release of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information**

1. Where the Commission or one of its departments determines that there is an exceptional need to release CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information to a third country, international organisation or an EU entity but no security of information agreement or administrative arrangement is in place, the exceptional *ad hoc* release procedure shall be followed.

<sup>(10)</sup> The table of equivalence for Member State markings is set out in Annex I to Decision (EU, Euratom) 2015/444.

2. Commission departments shall contact the Commission security authority, which shall consult the Commission Security Expert Group.
3. After consulting the Commission Security Expert Group, the Commission may, on the basis of a proposal by the member of the Commission responsible for security matters, authorise release of the information concerned.

## CHAPTER 6

### END OF LIFE FOR CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION

#### Article 37

##### **When to downgrade or declassify**

1. Information shall remain classified only for as long as it requires protection. Downgrading means a reduction in the level of security classification. Declassification means that the information shall no longer be considered as classified at all. At the time of its creation, the originator shall indicate, where possible, whether the EUCI can be downgraded or declassified on a given date or following a specific event. Otherwise, the originator shall review the information and assess the risks at least every 5 years in order to determine whether the original classification level is still appropriate.
2. Commission documents may also be downgraded or declassified on an *ad hoc* basis, for example following a request for access from the public.

#### Article 38

##### **Responsibility for downgrading and declassifying**

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall not be downgraded or declassified without the permission of the originator.
2. The Commission department that creates a classified document shall be responsible for deciding whether it can be downgraded or declassified. Within the Commission, all requests for downgrading and declassifying shall be subject to consultation of the Head of Unit or Director of the originating department. If the department has compiled classified information from various sources it shall first seek the consent of any other parties that provided source material, including in Member States, other EU bodies, third countries or international organisations.
3. Where the originating Commission department no longer exists and its responsibilities have been taken on by another service, the decision on downgrading and declassifying shall be taken by this service. Where the originating department no longer exists and its responsibilities have not been taken on by another service, the decision to downgrade or declassify shall be taken jointly by the Heads of Unit or Directors of the recipient Directorates-General.
4. The department responsible for downgrading or declassifying shall work with its respective registry on the practical arrangements for carrying out downgrading or declassification.

#### Article 39

##### **Sensitive non-classified information**

When reviewing a document results in a decision to declassify, consideration shall be given as to whether the document should bear a sensitive non-classified information distribution marking within the meaning of Article 9 of Decision (EU, Euratom) 2015/443.

#### Article 40

##### **How to indicate that a document has been downgraded or declassified**

1. The original classification marking at the top and bottom of every page shall be visibly crossed out (not removed) using the 'strikethrough' functionality for electronic formats, or manually for print-outs.
2. The first (cover) page shall be stamped as downgraded or declassified and completed with the details of the authority responsible for downgrading or declassifying and the corresponding date.

3. The original recipients of the CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be informed of the downgrading or declassification. The initial recipients shall be responsible for informing any subsequent addressees to whom they have sent or copied the original CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.
4. The Commission's Historical Archives Service shall be informed of all declassification decisions taken.
5. All translations of classified information shall be subject to the same downgrading or declassification procedures as the original language version.

#### Article 41

##### **Partial downgrading or declassification of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information**

1. Partial downgrading or declassification shall also be possible (e.g. annexes, some paragraphs only). The procedure shall be identical to that for downgrading or declassifying an entire document.
2. Upon partial declassification ('sanitising') of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information, a declassified extract shall be produced.
3. The parts that remain classified shall be replaced by:

**PART NOT TO BE DECLASSIFIED**

either in the body of the text itself, if the part that remains classified is a part of a paragraph, or as a paragraph, if the part that remains classified is a specific paragraph or more than one paragraph.

4. Specific mention shall be made in the text if a complete annex cannot be declassified and has therefore been withheld from the extract.

#### Article 42

##### **Routine destruction and deletion of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information**

1. The Commission shall not amass large quantities of classified information.
2. Originating departments shall review documents at least every 5 years for destruction or deletion. A review shall take place both for information stored on paper and for information stored in CIS at regular intervals.
3. Staff shall not destroy any hard copy CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents that they no longer require, but shall instead ask their Registry Control Officer to destroy the documents, subject to any archiving requirements for the original document.
4. Staff shall not be required to inform the originator if they delete copies of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET documents.
5. Draft material containing classified information shall be subject to the same disposal methods as finalised classified documents.
6. Only approved shredders shall be used for destroying CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents. Level 5 of DIN 66399 shredders are suitable for destroying CONFIDENTIEL UE/EU CONFIDENTIAL documents. Level 6 of DIN 66399 shredders are suitable for destroying SECRET UE/EU SECRET documents.
7. The shred from approved shredders may be disposed of as normal office waste.

8. The Registry Control Officer shall create destruction certificates and update the logbooks and other registration information accordingly.
9. All media and devices containing CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall be properly sanitised when they reach the end of their lifetime. The electronic data shall be destroyed or erased from information technology resources and associated storage media in a manner that gives reasonable assurance that the information cannot be recovered. Sanitisation shall remove data from the storage device, and also remove all labels, markings and activity logs.
10. Computer storage media shall be given to the LSO or Local Informatics Security Officer and/or Registry Control Officer for destruction and disposal.

#### Article 43

##### **Evacuation and destruction of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information in an emergency**

1. The Head of Department shall develop, approve and if necessary activate emergency evacuation and destruction plans to safeguard EUCI that is at significant risk of falling into unauthorised hands during a crisis. In order of priority, and depending on the nature of the emergency, consideration shall be given to:
  - (1) moving EUCI to an alternative safe place, where possible a Secured Area within the same building;
  - (2) evacuating EUCI to an alternative safe place, where possible a Secured Area in a different building, where possible a Commission building;
  - (3) destroying EUCI, where possible using the approved means of destruction.
2. When emergency plans have been activated, priority shall be given to moving or destroying SECRET UE/EU SECRET information first, and any CONFIDENTIEL UE/EU CONFIDENTIAL thereafter.
3. The operational details of emergency evacuation and destruction plans shall themselves be classified as RESTREINT UE/EU RESTRICTED. A copy shall be kept in each safe that stores CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information so as to be accessible in the event of an emergency.

#### Article 44

##### **Archiving**

1. Decisions on whether and when to archive, and the corresponding practical measures to be taken, shall be in accordance with the Commission's policy on document management.
2. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall not be sent to the Historical Archives of the European Union in Florence.

#### CHAPTER 7

##### **FINAL PROVISIONS**

#### Article 45

##### **Transparency**

This Decision shall be brought to the attention of Commission staff and to all individuals to whom it applies, and shall be published in the *Official Journal of the European Union*.

*Article 46***Entry into force**

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

Done at Brussels, 17 October 2019.

*For the Commission,*  
*On behalf of the President,*  
Günther OETTINGER  
*Member of the Commission*

---

## ANNEX

**Categories of staff who may have access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information if needed in order to perform their professional tasks**

| Categories of Commission personnel                                    | Access to C-UE/EU- C and S-UE/EU-S information | Conditions                                                                                                                                                        |
|-----------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Officials                                                             | Yes                                            | Vetting + briefing + acknowledge + authorisation + need-to-know                                                                                                   |
| Temporary agents                                                      | Yes                                            | Vetting + briefing + acknowledge + authorisation + need-to-know                                                                                                   |
| Contractual agents                                                    | Yes                                            | Vetting + briefing + acknowledge + authorisation + need-to-know                                                                                                   |
| Seconded national experts (SNEs)                                      | Yes                                            | Only when cleared by EU Member States prior to taking up their assignment + briefed by the Commission + acknowledge + authorised by the Commission + need-to-know |
| Trainees                                                              | No                                             | No exceptions possible                                                                                                                                            |
| Any other category of personnel (interim, intra-muros externals etc.) | No                                             | Consult the Commission security authority for any exceptions                                                                                                      |

**COMMISSION DECISION (EU, Euratom) 2019/1962**  
**of 17 October 2019**  
**on implementing rules for handling RESTREINT UE/EU RESTRICTED information**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on security in the Commission <sup>(1)</sup>,

Having regard to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information <sup>(2)</sup>,

Having regard to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission <sup>(3)</sup>,

Whereas:

- (1) Decision (EU, Euratom) 2015/444 applies to all Commission departments and in all premises of the Commission.
- (2) Security measures for protecting EU classified information (EUCI) throughout its life-cycle are to be commensurate in particular with its security classification.
- (3) Articles 4(3), 19(1)(c) and 22 of Decision (EU, Euratom) 2015/444 provide that more detailed provisions to supplement and support implementation of the Decision are to be laid down in implementing rules, governing issues such as a classification guide, compensatory measures for handling EUCI outside a Secured Area or an Administrative Area, and originator responsibilities.
- (4) Where necessary, implementing rules to supplement or support Decision (EU, Euratom) 2015/444 are to be adopted in accordance with Article 60 of that Decision.
- (5) Security measures taken to implement this Decision are to comply with the principles for security in the Commission set out in Article 3 of Decision (EU, Euratom) 2015/443.
- (6) The Council, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy have agreed to ensure maximum consistency in the application of security rules regarding their protection of EUCI while taking into account their specific institutional and organisational needs, in accordance with the declarations attached to the minutes of the Council session at which Council Decision 2013/488/EU <sup>(4)</sup>.
- (7) On 4 May 2016 the Commission adopted a decision <sup>(5)</sup> empowering the Member of the Commission responsible for security matters to adopt, on behalf of the Commission and under its responsibility, the implementing rules provided for in Article 60 of Decision (EU, Euratom) 2015/444,

<sup>(1)</sup> OJ L 72, 17.3.2015, p. 41.

<sup>(2)</sup> OJ L 72, 17.3.2015, p. 53.

<sup>(3)</sup> OJ L 6, 11.1.2017, p. 40.

<sup>(4)</sup> Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

<sup>(5)</sup> Commission Decision of 4 May 2016 on an empowerment relating to security [C(2016) 2797 final].

HAS ADOPTED THIS DECISION:

## CHAPTER 1

### GENERAL PROVISIONS

#### Article 1

##### **Subject matter and scope**

1. This Decision sets out the handling conditions for EU classified information (EUCI) of RESTREINT UE/EU RESTRICTED level <sup>(6)</sup> in compliance with Decision (EU, Euratom) 2015/444.
2. This Decision shall apply to all Commission departments and in all premises of the Commission.

#### Article 2

##### **Criteria for access to RESTREINT UE/EU RESTRICTED information**

1. Access to information classified as RESTREINT UE/EU RESTRICTED may be granted after:
  - (a) The need for an individual to have access to certain RESTREINT UE/EU RESTRICTED information in order to be able to perform a professional function or task for the European Commission has been determined;
  - (b) The individual has been briefed on the rules and the relevant security standards and guidelines for protecting RESTREINT UE/EU RESTRICTED information; and
  - (c) The individual has acknowledged their responsibilities for protecting the information concerned.
2. Commission trainees shall not be given duties that require them to have access to RESTREINT UE/EU RESTRICTED information.
3. Access shall be withheld or permitted for other categories of staff in accordance with the table set out in the Annex.

## CHAPTER 2

### CREATING RESTREINT UE/EU RESTRICTED INFORMATION

#### Article 3

##### **Originator**

While the originator within the meaning of Article 1 of Decision (EU, Euratom) 2015/444 is the Union institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the Union's structures, the drafter of RESTREINT UE/EU RESTRICTED information will not necessarily be the same.

#### Article 4

##### **Assigning a classification level**

1. Staff drafting a document on the basis of information within the meaning of Article 1 shall always consider whether their document needs to be classified. Classifying a document as EUCI shall involve an assessment and a decision by the originator as to whether the disclosure of the document to unauthorised persons would cause prejudice to the interests of the European Union or of one or more of the Member States. If drafters are in any doubt as to whether the document they are drafting warrants being classified as RESTREINT UE/EU RESTRICTED they should consult the Head of Unit or Director responsible.
2. A document shall be classified as at least RESTREINT UE/EU RESTRICTED if its unauthorised disclosure could, inter alia:
  - (a) adversely affect diplomatic relations;
  - (b) cause substantial distress to individuals;

<sup>(6)</sup> Pursuant to Article 3 of Decision (EU, Euratom) 2015/444, RESTREINT UE/EU RESTRICTED information shall mean 'information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States'.

- (c) make it more difficult to maintain the operational effectiveness or security of Member States' or other contributors' deployed personnel;
- (d) breach undertakings to maintain the confidence of information provided by third parties;
- (e) prejudice the investigation of or facilitate crime;
- (f) disadvantage the Union or Member States in commercial or policy negotiations with others;
- (g) impede the effective development or operation of Union policies;
- (h) undermine the proper management of the Union and its missions in general; or
- (i) lead to the discovery of information classified at a higher level.

3. Originators may decide to attribute a standard classification level to categories of information that they create on a regular basis. However, they shall ensure that individual pieces of information are given the appropriate classification level.

#### *Article 5*

##### **Working with drafts**

1. Information shall be classified as soon as it is produced. Personal notes, preliminary drafts or messages containing information that warrants classification at the level of RESTREINT UE/EU RESTRICTED shall be marked as such from the outset and shall be produced and handled in accordance with this Decision.

2. If the final document no longer warrants the RESTREINT UE/EU RESTRICTED classification level it shall be declassified.

#### *Article 6*

##### **Record of source material**

In order to enable the exercise of originator control in accordance with Article 13, originators of RESTREINT UE/EU RESTRICTED documents shall, to the extent possible, keep a record of any classified sources used for producing classified documents, including details of sources originally from EU Member States, international organisations or third countries. Where appropriate, aggregated classified information shall be marked in such a way as to preserve the identification of the originators of the classified source materials used.

#### *Article 7*

##### **Classifying parts of a document**

1. In accordance with Article 22(6) of Decision (EU, Euratom) 2015/444, the overall classification level of a document shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final aggregated document shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

2. Documents containing classified and non-classified parts shall be structured and marked so that components with different classification and/or sensitivity levels can be easily identified and detached if necessary. This shall enable each part to be handled appropriately when detached from the other components.

#### *Article 8*

##### **Full classification marking**

1. Information that warrants classification shall be marked and handled as such regardless of its physical form. The classification level shall be clearly communicated to recipients, either by a classification marking, if the information is delivered in written form, whether this is on paper, on removable storage media or in a Communication and Information System (CIS), or by an announcement, if the information is delivered in oral form, such as in a conversation or a presentation. Classified material shall be physically marked so as to allow for easy identification of its security classification.

2. On documents, the full classification marking RESTREINT UE/EU RESTRICTED shall be written in block capitals, in full in French and English (French first), in accordance with paragraph 3. The marking shall not be translated into other languages.
3. The RESTREINT UE/EU RESTRICTED classification marking shall be affixed as follows:
  - (a) centred at the top and bottom of every page of the document;
  - (b) the complete classification marking on one line, with no spaces either side of the forward slash;
  - (c) in capitals, black, font Times New Roman 16, bold and surrounded by a border on each side.
4. When creating a RESTREINT UE/EU RESTRICTED 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 itself shall not be classified information unless it is marked as such;
  - (d) all the annexes and enclosures shall be listed, whenever possible on the first page; and
  - (e) the document shall have the date of its creation on it.

#### Article 9

##### Abbreviated R-UE/EU-R classification marking

The abbreviation R-UE/EU-R may be used to indicate the classification level of individual parts of a RESTREINT UE/EU RESTRICTED document or where the full classification marking cannot be inserted, for example on a small removable storage medium. It may be used in the body of text where repeated use of the full classification marking is cumbersome. The abbreviation shall not be used instead of the full classification markings in the header and footer of the document.

#### Article 10

##### Other security designators

1. RESTREINT UE/EU RESTRICTED documents may bear other markings, or 'security designators', specifying, for example, the field to which the document relates, or indicating a particular distribution on a need-to-know basis. An example is:

**RELEASABLE TO LIECHTENSTEIN**

2. RESTREINT UE/EU RESTRICTED documents may bear a security caveat that gives specific instructions on how to handle and manage the documents.

3. Whenever possible, any indications for declassifying shall be affixed on the first page of the document at the time it is created. For example, the following marking may be used:

**RESTREINT UE/EU RESTRICTED**

until [dd.mm.yyyy]

#### Article 11

##### Electronic processing

1. RESTREINT UE/EU RESTRICTED documents shall be created using electronic means, where these are available.

2. Commission staff shall use accredited CIS for creating RESTREINT UE/EU RESTRICTED level information. Staff shall consult their Local Security Officer (LSO) if there is any doubt as to which CIS may be used. In consultation with the Commission security authority specific procedures may be applied in emergencies or in specific technical configurations.

3. RESTREINT UE/EU RESTRICTED documents, including drafts, as required by Article 5, shall not be sent by ordinary open email, printed or scanned on standard printers or scanners, or handled on the personal devices of members of staff. Only printers or copiers connected to standalone computers or to an accredited system shall be used to print out RESTREINT UE/EU RESTRICTED documents.

#### *Article 12*

##### **Distribution**

The sender of RESTREINT UE/EU RESTRICTED documents shall decide who to distribute the information to, based on their need-to-know. If required a distribution list shall be drawn up in order to further enforce the need-to-know principle.

#### CHAPTER 3

##### **WORKING WITH EXISTING RESTREINT UE/EU RESTRICTED INFORMATION**

#### *Article 13*

##### **Originator control**

1. The originator shall have 'originator control' over RESTREINT UE/EU RESTRICTED information which it has created. The originator's prior written consent shall be sought before the information can be:

- (a) declassified;
- (b) used for purposes other than those established by the originator;
- (c) released to a third country or international organisation;
- (d) disclosed to a party outside the Commission but within the EU; or
- (e) disclosed to a contractor or prospective contractor located in a third country.

2. Holders of RESTREINT UE/EU RESTRICTED information have been given access to the classified information in order to be able to perform their duties. They are responsible for the correct handling, storage and protection of it in accordance with Decision (EU, Euratom) 2015/444. Unlike originators of classified information, holders shall not be authorised to decide on the declassification or onward release of RESTREINT UE/EU RESTRICTED information to third countries or international organisations.

3. If the originator of a piece of RESTREINT UE/EU RESTRICTED information cannot be identified, the Commission department holding that classified information shall exercise originator control. The Commission Security Expert Group shall be consulted before RESTREINT UE/EU RESTRICTED information is released to a third country or international organisation.

#### *Article 14*

##### **CIS suitable for handling RESTREINT UE/EU RESTRICTED information**

RESTREINT UE/EU RESTRICTED information shall be handled and transmitted by electronic means, where these are available. Only CIS and equipment that has been accredited by the Commission security accreditation authority shall be used.

*Article 15***Specific measures for RESTREINT UE/EU RESTRICTED information on removable storage media**

1. The use of removable storage media shall be controlled and accounted for. Only removable storage media provided by the Commission and encrypted by a product approved by the Commission security authority shall be used. Personal removable storage media and those given freely at conferences, seminars, etc. shall not be used for transferring classified information. Where possible, Tempest-proof removable storage media should be used, in accordance with the guidance from the Commission security authority.
2. Where a classified document is handled or stored electronically on removable storage media, such as USB sticks, CDs or memory cards, the classification marking shall be clearly visible on the displayed information itself, as well as in the filename and on the removable storage medium.
3. Staff shall bear in mind that when large amounts of classified information are stored on removable storage media the device may warrant a higher classification level.
4. Only CIS that have been appropriately accredited shall be used to transfer RESTREINT UE/EU RESTRICTED information onto or from removable storage media.
5. When downloading RESTREINT UE/EU RESTRICTED information on removable storage media, particular care shall be taken to ensure that the media does not contain viruses or malware prior to the transfer of the data.
6. Where applicable, removable storage media shall be handled in accordance with any security operating procedures relating to the encryption system used.
7. Documents on removable storage media that are either no longer required, or have been transferred onto an appropriate CIS, shall be securely removed or deleted using approved products or methods. Unless stored in appropriate locked office furniture, removable storage media shall be destroyed when no longer needed. Any destruction or deletion shall use a method that is in accordance with the Commission security rules. An inventory shall be kept of the removable media, and their destruction shall be recorded.

*Article 16***Handling and storage of RESTREINT UE/EU RESTRICTED information**

1. In accordance with Article 19(1)(a) and (b) of Decision (EU, Euratom) 2015/444, RESTREINT UE/EU RESTRICTED information may be handled in an Administrative Area or in a Secured Area <sup>(7)</sup> as follows:
  - staff shall close the office door when handling RESTREINT UE/EU RESTRICTED information,
  - staff shall stow any RESTREINT UE/EU RESTRICTED information away or cover it should they receive a visitor,
  - staff shall not leave RESTREINT UE/EU RESTRICTED information visible when the office is unoccupied,
  - screens displaying RESTREINT UE/EU RESTRICTED information shall be permanently turned away from windows and doors to prevent potential overlooking.

<sup>(7)</sup> As defined in Article 18 of Decision (EU, Euratom) 2015/444.

2. In accordance with Article 19(1)(c) of Decision (EU, Euratom) 2015/444, RESTREINT UE/EU RESTRICTED information may be handled outside a Secured Area or an Administrative Area, provided the holder has undertaken to comply with compensatory measures to protect it from access by unauthorised persons. The compensatory measures shall include at least the following:

- RESTREINT UE/EU RESTRICTED information shall not be read in public places,
- the EUCI shall be kept at all times under the personal control of the holder,
- the documents shall be stowed in appropriate locked furniture when they are not being read or discussed,
- the doors to the room shall be closed while the document is being read or discussed,
- the details of the document shall not be discussed over the phone on a non-secured line or in an unencrypted email,
- the document may only be photocopied or scanned on stand-alone or accredited equipment,
- the document shall only be handled and temporarily held outside an Administrative or Secured Area for the minimum time necessary,
- the holder shall not throw the classified document away but shall return it for storage in an Administrative or Secured Area, or ensure it is destroyed in an approved shredder.

3. Hard copy RESTREINT UE/EU RESTRICTED information shall be stored in locked office furniture in an Administrative Area or in a Secured Area. It may be stored temporarily outside a Secured Area or an Administrative Area provided the holder has undertaken to comply with compensatory measures.

4. Further advice can be sought from the Local Security Officer (LSO) of the relevant Commission department.

5. Any suspected or actual security incidents involving the document shall be reported to the LSO as soon as possible.

#### *Article 17*

##### **Copying and translating RESTREINT UE/EU RESTRICTED information**

1. RESTREINT UE/EU RESTRICTED information may be copied or translated on instruction from the holder, provided the originator has not imposed any caveats. However, no more copies shall be made than are strictly necessary.

2. Where only part of a classified document is reproduced, the same conditions shall apply as for copying the full document. Extracts shall also be classified as RESTREINT UE/EU RESTRICTED, unless the originator has specifically marked them as unclassified.

3. The security measures applicable to the original information shall also be applied to copies and translations thereof.

#### *Article 18*

##### **General principles for carrying RESTREINT UE/EU RESTRICTED information**

1. Whenever possible, RESTREINT UE/EU RESTRICTED information that needs to be taken outside Secured Areas or Administrative Areas shall be sent electronically by appropriately accredited means and/or protected by approved cryptographic products.

2. Depending on the means available or the particular circumstances, RESTREINT UE/EU RESTRICTED information may be physically carried by hand in the form of paper documents or on removable storage media. The use of removable storage media to transfer RESTREINT UE/EU RESTRICTED information shall be given preference to sending paper documents.
3. Only removable storage media encrypted by a product approved by the Commission security authority may be used. RESTREINT UE/EU RESTRICTED information on removable storage media that is not protected by an encryption product that has been approved by the Commission security authority shall be handled in the same manner as paper copy.
4. A consignment may contain more than one piece of RESTREINT UE/EU RESTRICTED information, provided the need-to-know principle is respected.
5. The packaging used shall ensure that the contents are covered from view. RESTREINT UE/EU RESTRICTED information shall be carried in opaque packaging, such as an envelope, an opaque folder or a briefcase. The outside of the packaging shall not bear any indication of the nature or classification level of its contents. If used, the inner layer of packaging shall be marked as RESTREINT UE/EU RESTRICTED. Both layers shall state the intended recipient's name, job title and address, as well as a return address in case delivery cannot be made.
6. Any security incidents involving RESTREINT UE/EU RESTRICTED information that is carried by staff or couriers shall be reported for subsequent investigation to the Security Directorate of the Directorate-General for Human Resources, via the LSO of the relevant Commission department.

#### *Article 19*

##### **Hand carriage of removable storage media**

1. Removable storage media that are used to transport RESTREINT UE/EU RESTRICTED information shall be accompanied by a dispatch note, detailing the removable storage media containing the classified information, as well as all files contained on them, to allow the recipient to make the necessary verifications.
2. Only the documents to be provided shall be stored on the media. All the classified information on a single USB stick, for instance, would have to be intended for the same recipient. The sender shall bear in mind that large amounts of classified information stored on such devices may warrant a higher classification level for the device as a whole.
3. Only removable storage media bearing the appropriate classification marking shall be used to carry RESTREINT UE/EU RESTRICTED information.

#### *Article 20*

##### **Carriage of RESTREINT UE/EU RESTRICTED documents within Commission buildings**

1. Staff may carry RESTREINT UE/EU RESTRICTED documents within a Commission building, but the documents shall not leave the possession of the bearer or be read in public.
2. RESTREINT UE/EU RESTRICTED documents may be sent through internal mail to other European Commission offices in a single ordinary opaque envelope, but with no indication on the outside that the contents are classified. Other EU institutions or bodies served directly by the Commission's internal mail system may also be sent RESTREINT UE/EU RESTRICTED documents in the same way.

#### *Article 21*

##### **Carriage of RESTREINT UE/EU RESTRICTED documents within the Union**

1. RESTREINT UE/EU RESTRICTED information may be carried by staff or Commission couriers anywhere within the Union provided they comply with the following instructions:
  - (a) an opaque envelope or packaging shall be used to convey RESTREINT UE/EU RESTRICTED information. The outside shall not bear any indication of the nature or classification level of its contents;

- (b) the RESTREINT UE/EU RESTRICTED information shall not leave the possession of the bearer; and
- (c) the envelope or package shall not be opened *en route* and the information shall not be read in public places.

2. Staff wishing to send RESTREINT UE/EU RESTRICTED information to other locations in the Union may arrange for it to be conveyed by one of the following means:

- by national postal services that track the consignment or certain commercial courier services that guarantee personal hand carriage, provided that they meet the requirements set out in Article 23 of this Decision,
- by military, government or diplomatic courier, in coordination with Registry staff.

#### Article 22

##### **Carriage of RESTREINT UE/EU RESTRICTED information from or to the territory of a third country**

1. Information classified as RESTREINT UE/EU RESTRICTED may be hand-carried by staff between the territory of the Union and the territory of a third country.
2. Registry staff may arrange for one of the following:
  - carriage by postal services that track the consignment or commercial courier services that guarantee personal hand carriage,
  - carriage by military or diplomatic courier.
3. When hand-carrying either paper documents or removable storage media classified as RESTREINT UE/EU RESTRICTED, staff shall comply with all of the following additional measures:
  - when travelling by public transport the classified information shall be placed in a briefcase or bag that is kept in the bearer's personal custody. It shall not be consigned to a baggage hold,
  - the RESTREINT UE/EU RESTRICTED information shall be conveyed inside two layers of packaging. The inner layer of packaging shall bear an official seal to indicate that it is an official consignment and is not to undergo security scrutiny,
  - the bearer shall carry a courier certificate, which certifies that the bearer is authorised to carry the RESTREINT UE/EU RESTRICTED consignment, issued by the relevant department's registry.

#### Article 23

##### **Transport by commercial couriers**

1. For the purposes of this Decision, 'commercial couriers' include national postal services and commercial courier companies that offer a service where information is delivered for a fee and is either personally hand carried or tracked.
2. Commercial couriers may use the services of a sub-contractor. However, responsibility for complying with this Decision shall remain with the courier company.
3. If the intended recipient is outside the EU, two layer of packaging shall be used. When classified consignments are being prepared the sender shall bear in mind that commercial courier services shall only deliver RESTREINT UE/EU RESTRICTED consignments to the intended recipient, a duly authorised substitute, the registry control officer or his/her duly authorised substitute or a receptionist. To mitigate the risk that the consignment may not reach the intended recipient, the outer and, where applicable the inner, layer of packaging of the consignment shall bear a return address.

4. Services offered by commercial couriers providing electronic transmission of registered delivery documents shall not be used for RESTREINT UE/EU RESTRICTED information.

#### *Article 24*

##### **Other specific handling conditions**

1. Any carriage conditions set out in a security of information agreement or in administrative arrangements shall be complied with. If in doubt, staff shall consult their respective registry or the Security Directorate in the Directorate-General for Human Resources and Security.
2. The double packaging requirement can be waived for classified information that is protected by approved cryptographic products. However, for addressing purposes, and also as the removable storage medium bears an explicit security classification marking, the medium shall be carried in at least an ordinary envelope but may require additional physical protection measures, such as bubble wrap envelopes.

#### CHAPTER 4

##### **CLASSIFIED MEETINGS**

#### *Article 25*

##### **Preparing for a RESTREINT UE/EU RESTRICTED meeting**

1. Meetings where RESTREINT UE/EU RESTREINT information is due to be discussed shall only be held in a meeting room that has been accredited at the appropriate level or higher. Where these are not available, staff shall seek the advice of the Commission security authority.
2. As a general rule, agendas should be not classified. If the agenda of a meeting mentions classified documents, the agenda itself shall not automatically be 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.
3. If electronic files containing RESTREINT UE/EU RESTRICTED information are to be attached to the agenda, it is mandatory to protect them with cryptographic products approved by the Commission Crypto Authority.
4. Meeting organisers shall remind participants that any comments sent in on a RESTREINT UE/EU RESTRICTED agenda item must not be sent through ordinary open e-mails, or through other means that have not been appropriately accredited in accordance with Article 11 of this Decision.
5. Meeting organisers shall endeavour to group RESTREINT UE/EU RESTRICTED items consecutively on the agenda in order to facilitate the smooth functioning of the meeting. Only persons with a need-to-know may be present during discussions of classified items.
6. The invitation itself shall forewarn the participants that the meeting will discuss classified topics, and that corresponding security measures will apply.
7. The invitation or note on the agenda itself shall remind participants that portable electronic devices are to be switched off during discussion of RESTREINT UE/EU RESTRICTED items.
8. Meeting organisers shall prepare a complete list of external participants prior to the meeting.

#### *Article 26*

##### **Electronic equipment in a RESTREINT UE/EU RESTRICTED meeting room**

1. Only accredited IT systems in accordance with Article 11 of this Decision may be used where classified information is conveyed, such as to give a presentation that displays RESTRICTED EU/EU RESTRICTED information, or for videoconferences.
2. The Chair shall ensure that unauthorised portable electronic devices have been switched off.

*Article 27***Procedures to be followed during a RESTREINT UE/EU RESTRICTED meeting**

1. At the start of the classified discussion, the Chair shall announce to the meeting that it is moving into classified mode. The doors and blinds shall be closed.
2. Only the necessary number of documents shall be given to participants and interpreters, as appropriate, at the start of the discussion.

RESTREINT UE/EU RESTRICTED documents shall not be left unattended during any breaks in the meeting.

3. At the end of the meeting, the participants and interpreters shall be reminded not to leave any classified documents or classified notes they might have made lying unattended in the room. Classified documents or notes not taken away by the participants at the end of the meeting shall be collected by the meeting organisers and shredded in appropriate shredders.

4. The list of participants and an outline of any classified information shared with Member States and released orally to third countries or international organisations shall be noted down during the meeting in order to be recorded in the outcome of proceedings.

*Article 28***Interpreters and translators**

Only interpreters and translators who are subject to the Staff regulations or the Conditions of Employment of other servants of the European Union or who have a contractual link to the Commission shall have access to RESTREINT UE/EU RESTRICTED information.

## CHAPTER 5

**SHARING AND EXCHANGING RESTREINT UE/EU RESTRICTED INFORMATION***Article 29***Originator consent**

If the Commission is not the originator of the classified information for which release or sharing is desired, or of the source material it may contain, the Commission department which holds this classified information shall first seek the originator's written consent to release. If the originator cannot be identified, the Commission department holding that classified information shall exercise originator control.

*Article 30***Sharing RESTREINT UE/EU RESTRICTED information with other Union entities**

1. RESTREINT UE/EU RESTRICTED information shall only be shared with another Union institution, agency, body or office if the recipient has a need-to-know and the entity has a corresponding legal arrangement with the Commission.
2. Within the Commission, the EUCI Registry managed by the Secretariat-General shall as a general rule be the main point of entry and exit for classified information exchanges with other Union institutions, agencies, bodies and offices. However, RESTREINT UE/EU RESTRICTED information may be shared directly with intended recipients.

*Article 31***Exchanging RESTREINT UE/EU RESTRICTED information with Member States**

1. RESTREINT UE/EU RESTRICTED information may be shared with Member States if the recipient has a need-to-know.

2. Member States' classified information that bears an equivalent national classification marking <sup>(8)</sup> and which has been provided to the Commission shall be afforded the same level of protection as RESTREINT UE/EU RESTRICTED information.

#### Article 32

##### **Exchanging RESTREINT UE/EU RESTRICTED information with third countries and international organisations**

1. RESTREINT UE/EU RESTRICTED information shall only be released to a third country or international organisation if the recipient has a need-to-know and the country or international organisation has an appropriate legal or administrative framework in place, such as a security of information agreement or an administrative arrangement with the Commission. The provisions of such an agreement or arrangement shall prevail over the provisions of this Decision.

2. The EUCI registry managed by the Secretariat-General shall as a general rule act as the main point of entry and exit for all information classified RESTREINT UE/EU RESTRICTED exchanged between the Commission and third countries and international organisations. The Commission security authority shall be consulted where there are security, organisational or operational grounds which make it more appropriate for local EUCI registries to operate as the point of entry and exit for matters within the competence of the department concerned.

3. To ensure traceability, RESTREINT UE/EU RESTRICTED information shall be recorded:

— when it arrives in or leaves an organisational entity, and

— when it arrives in or leaves a CIS.

4. Such recording may be carried out on paper or in electronic logbooks.

5. Recording procedures for classified information handled within an accredited CIS may be performed by processes within the CIS itself. In that case, the CIS shall include measures to guarantee the integrity of the log records.

6. Classified information received from third countries or international organisations shall be afforded an equivalent level of protection as EUCI bearing the equivalent classification marking as set out in the respective security of information agreement or administrative arrangement.

#### Article 33

##### **Exceptional ad hoc release of RESTREINT UE/EU RESTRICTED information**

1. Where the Commission or one of its departments determines that there is an exceptional need to release RESTREINT UE/EU RESTRICTED information to a third country, international organisation or an EU entity but no security of information agreement or administrative arrangement is in place, the exceptional *ad hoc* release procedure shall be followed.

2. Commission departments shall contact the Commission security authority, which shall consult the Commission Security Expert Group.

3. After consulting the Commission Security Expert Group, the Commission may, on the basis of a proposal by the member of the Commission responsible for security matters, authorise release of the information concerned.

---

<sup>(8)</sup> The table of equivalence for Member State markings is set out in Annex I to Decision (EU, Euratom) 2015/444.

## CHAPTER 6

**END OF LIFE FOR RESTREINT UE/EU RESTRICTED INFORMATION***Article 34***When to declassify**

1. Information shall remain classified only for as long as it requires protection. Declassification means that the information shall no longer be considered as classified at all. At the time of its creation, the originator shall indicate, where possible, whether the EUCI can be declassified on a given date or following a specific event. Otherwise, the originator shall regularly review RESTREINT UE/EU RESTRICTED information to determine whether classification is still appropriate.
2. Information classified RESTREINT UE/EU RESTRICTED that has originated in the Commission will be automatically declassified after thirty years, in accordance with Regulation (EEC, Euratom) No 354/83 as amended by Council Regulation (EC, Euratom) No 1700/2003 <sup>(9)</sup>, and in accordance with Article 59(2)a of Decision (EU, Euratom) 2015/444.
3. Commission documents may also be declassified on an *ad hoc* basis, for example following a request for access from the public.

*Article 35***Responsibility for declassifying**

1. RESTREINT UE/EU RESTRICTED information shall not be declassified without the permission of the originator.
2. The Commission department that creates a classified document shall be responsible for deciding whether it can be declassified. Within the Commission, all requests for declassifying shall be subject to consultation of the Head of Unit or Director of the originating department. If the department has compiled classified information from various sources it shall first seek the consent of any other parties that provided source material, including in Member States, other EU bodies, third countries or international organisations.
3. Where the originating Commission department no longer exists and its responsibilities have been taken on by another service, the decision on declassifying shall be taken by this service. Where the originating department no longer exists and its responsibilities have not been taken on by another service, the decision to declassify shall be taken jointly by the Heads of Unit or Directors of the recipient Directorates-General.

*Article 36***Sensitive non-classified information**

When reviewing a document results in a decision to declassify, consideration shall be given as to whether the document should bear a sensitive non-classified information distribution marking within the meaning of Article 9 of Decision (EU, Euratom) 2015/443.

*Article 37***How to indicate that a document has been declassified**

1. The original classification marking at the top and bottom of every page shall be visibly crossed out (not removed) using the 'strikethrough' functionality for electronic formats, or manually for print-outs.
2. The first (cover) page shall be stamped as declassified and completed with the details of the authority responsible for declassifying and the corresponding date.

---

<sup>(9)</sup> Council Regulation (EC, Euratom) No 1700/2003 of 22 September 2003 amending Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 243, 27.9.2003, p. 1).

3. The original recipients of the RESTREINT UE/EU RESTRICTED information shall be informed of the declassification. The initial recipients shall be responsible for informing any subsequent addressees to whom they have sent or copied the original RESTREINT UE/EU RESTRICTED information.
4. The Commission's Historical Archives Service shall be informed of all declassification decisions taken.
5. All translations of classified information shall be subject to the same declassification procedures as the original language version.

#### Article 38

##### **Partial declassification of RESTREINT UE/EU RESTRICTED information**

1. Partial declassification shall also be possible (e.g. annexes, some paragraphs only). The procedure shall be identical to that for declassifying an entire document.
2. Upon partial declassification ('sanitising') of RESTREINT UE/EU RESTRICTED information, a declassified extract shall be produced.
3. The parts that remain classified shall be replaced by:

**PART NOT TO BE DECLASSIFIED**

either in the body of the text itself, if the part that remains classified is a part of a paragraph, or as a paragraph, if the part that remains classified is a specific paragraph or more than one paragraph.

4. Specific mention shall be made in the text if a complete annex cannot be declassified and has therefore been withheld from the extract.

#### Article 39

##### **Routine destruction and deletion of RESTREINT UE/EU RESTRICTED information**

1. The Commission shall not amass large quantities of classified information.
2. Originating departments shall routinely review small amounts for destruction or deletion at short intervals. A review shall take place both for information stored on paper and for information stored in CIS at regular intervals.
3. Staff shall destroy or securely delete any RESTREINT UE/EU RESTRICTED documents that are no longer required, subject to any archiving requirements for the original document.
4. Staff shall not be required to inform the originator if they destroy or delete copies of RESTREINT UE/EU RESTRICTED documents.
5. Draft material containing classified information shall be subject to the same disposal methods as finalised classified documents.
6. Only approved shredders shall be used for destroying RESTREINT UE/EU RESTRICTED documents. Level 4 of DIN 32757 and Level 5 of DIN 66399 shredders are suitable for destroying RESTREINT UE/EU RESTRICTED documents.
7. The shred from approved shredders may be disposed of as normal office waste.
8. All media and devices containing RESTREINT UE/EU RESTRICTED information shall be properly sanitised when they reach the end of their lifetime. The electronic data shall be destroyed or erased from information technology resources and associated storage media in a manner that gives reasonable assurance that the information cannot be recovered. Sanitisation shall remove data from the storage device, and also remove all labels, markings and activity logs.

9. Computer storage media shall be given to the LSO or Local Informatics Security Officer and/or Registry Control Officer for destruction and disposal.

#### *Article 40*

##### **Evacuation and destruction of RESTREINT UE/EU RESTRICTED information in an emergency**

1. The Head of Department shall develop, approve and if necessary activate emergency evacuation and destruction plans to safeguard RESTREINT UE/EU RESTRICTED information that is at significant risk of falling into unauthorised hands during a crisis. In order of priority, and depending on the nature of the emergency, consideration shall be given to:

- (1) moving EUCI to an alternative safe place, where possible an Administrative or Secured Area within the same building;
- (2) evacuating EUCI to an alternative safe place, where possible an Administrative or Secured Area in a different building, where possible, a Commission building;
- (3) destroying EUCI, where possible using the approved means of destruction.

2. When emergency plans have been activated, priority shall be given to moving or destroying higher levels of information first.

3. The operational details of emergency evacuation and destruction plans shall themselves be classified as RESTREINT UE/EU RESTRICTED.

#### *Article 41*

##### **Archiving**

1. Decisions on whether and when to archive, and the corresponding practical measures to be taken, shall be in accordance with the Commission's policy on document management.
2. RESTREINT UE/EU RESTRICTED documents shall not be sent to the Historical Archives of the European Union in Florence.

#### CHAPTER 7

#### **FINAL PROVISIONS**

#### *Article 42*

##### **Transparency**

This Decision shall be brought to the attention of Commission staff and to all individuals to whom it applies, and shall be published in the *Official Journal of the European Union*.

#### *Article 43*

##### **Entry into force**

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

Done at Brussels, 17 October 2019.

*For the Commission,*  
*On behalf of the President,*  
Günther OETTINGER  
*Member of the Commission*

## ANNEX

**Categories of staff who may have access to RESTREINT UE/EU RESTRICTED information if needed in order to perform their professional tasks**

| Categories of Commission personnel                                    | Access to R-UE/EU- R information | Conditions                                                   |
|-----------------------------------------------------------------------|----------------------------------|--------------------------------------------------------------|
| Officials                                                             | Yes                              | Briefing + acknowledge + need-to-know                        |
| Temporary agents                                                      | Yes                              | Briefing + acknowledge + need-to-know                        |
| Contractual agents                                                    | Yes                              | Briefing + acknowledge + need-to-know                        |
| Seconded national experts (SNEs)                                      | Yes                              | Briefing (by the Commission) + acknowledge + need-to-know    |
| Trainees                                                              | No                               | No exceptions possible                                       |
| Any other category of personnel (interim, intra-muros externals etc.) | No                               | Consult the Commission security authority for any exceptions |

**COMMISSION DECISION (EU, Euratom) 2019/1963****of 17 October 2019****laying down implementing rules on industrial security with regard to classified procurement contracts**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission <sup>(1)</sup>,

Having regard to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information <sup>(2)</sup>,

Having regard to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission <sup>(3)</sup>,

After consulting the Commission Security Expert Group, in accordance with Article 41(5) of Decision (EU, Euratom) 2015/444,

Whereas:

- (1) Articles 41, 42, 47 and 48 of Decision (EU, Euratom) 2015/444 provide that more detailed provisions to supplement and support Chapter 6 of that Decision are to be laid down in implementing rules on industrial security, governing issues such as tendering, conclusion of classified contracts, facility security clearances, personnel security clearances, visits and transmission and carriage of European Union classified information (EUCI).
- (2) Decision (EU, Euratom) 2015/444 states that classified contracts are to be implemented in close cooperation with the national security authority, the designated security authority or any other competent authority of the Member States concerned; the Member States have agreed to ensure that any entity under their jurisdiction which may receive or generate classified information originating in the Commission is appropriately security cleared and is capable of providing suitable protection equivalent to that afforded by the security rules of the Council of the European Union for protecting EU classified information bearing a corresponding classification marking, as provided in Agreement between the Member States of the European Union, meeting within Council, regarding the protection of classified information exchanged in the interests of the European Union (2011/C 202/05) <sup>(4)</sup>.
- (3) The Council, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy have agreed to ensure maximum consistency in the application of security rules regarding their protection of EUCI while taking into account their specific institutional and organisational needs, in accordance with the declarations attached to the minutes of the Council session at which Council Decision 2013/488/EU <sup>(5)</sup> on the security rules for protecting EU classified information was adopted.
- (4) The Commission's implementing rules on industrial security with regard to classified contracts should therefore also ensure maximum consistency and take into account the Guidelines on Industrial Security approved by the Council Security Committee on 13 December 2016 and Articles 7 and 22 of Directive 2009/81/EC of the European Parliament and of the Council <sup>(6)</sup>.
- (5) On 4 May 2016 the Commission adopted a decision <sup>(7)</sup> empowering the Member of the Commission responsible for security matters to adopt, on behalf of the Commission and under its responsibility, the implementing rules provided for in Article 60 of Decision (EU, Euratom) 2015/444,

<sup>(1)</sup> OJ L 72, 17.3.2015, p. 41.

<sup>(2)</sup> OJ L 72, 17.3.2015, p. 53.

<sup>(3)</sup> OJ L 6, 11.1.2017, p. 40.

<sup>(4)</sup> OJ C 202, 8.7.2011, p. 13.

<sup>(5)</sup> Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

<sup>(6)</sup> Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security (OJ L 216, 20.8.2009, p. 76).

<sup>(7)</sup> Commission Decision of 4 May 2016 on an empowerment relating to security (C(2016) 2797 final).

HAS ADOPTED THIS DECISION:

## CHAPTER 1

### GENERAL PROVISIONS

#### Article 1

##### Subject matter and scope

1. This Decision sets out implementing rules on industrial security with regard to classified procurement contracts to support the implementation of Decision (EU, Euratom) 2015/444, and in particular Chapter 6 of that Decision.
2. This Decision lays down specific requirements to ensure the protection of EU classified information (EUCI) by economic operators in pre-contract stage, throughout the life cycle of classified contracts concluded by the European Commission, and in subcontracts concluded by Commission contractors.
3. This Decision concerns information classified at the following levels:
  - (a) RESTREINT UE/EU RESTRICTED;
  - (b) CONFIDENTIEL UE/EU CONFIDENTIAL;
  - (c) SECRET UE/EU SECRET.

#### Article 2

##### Responsibility within the Commission

1. As part of the responsibilities as described in the Financial Regulation <sup>(8)</sup>, each authorising officer of the Commission contracting authority shall ensure that the classified contract refers to the minimum standards on industrial security set out in Chapter 6 of Decision (EU, Euratom) 2015/444 and in these implementing rules, and where appropriate in the contract notice or the invitation to tender, and that these standards are met in the course of implementation.
2. To that end, the authorising officer concerned shall, at all stages, seek the advice of the Commission security authority on issues regarding the security elements of a classified contract, programme or project, and shall inform the local security officer about the contracts concluded. The decision on the classification level of specific subjects shall rest with the contracting authority and shall be taken with due regard to the security classification guide.
3. In respecting the requirements of these implementing rules, the Commission security authority shall cooperate closely with the national security authorities (NSAs) and the designated security authorities (DSAs) of the Member States concerned, in particular as regards facility security clearances (FSCs) and personnel security clearances (PSCs), visit procedures and transportation plans.

## CHAPTER 2

### HANDLING OF CALLS FOR TENDER FOR CLASSIFIED CONTRACTS

#### Article 3

##### Basic principles

1. Classified contracts shall be awarded only to economic operators registered in a Member State, or to economic operators registered in a third country or established by an international organisation where that third country or international organisation has concluded a security of information agreement with the European Union or entered into an administrative arrangement with the Commission <sup>(9)</sup>.
2. Before launching an invitation to tender for a classified contract, the contracting authority shall determine the security classification of any information that could be provided to tenderers. The contracting authority shall also determine the maximum security classification of any information generated in the performance of the contract or programme or project, or at least the anticipated volume and type of information to be produced or handled, and the need for a classified communication and information system (CIS).

<sup>(8)</sup> Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

<sup>(9)</sup> The list of agreements concluded by the EU and of administrative arrangements entered into by the European Commission, under which EU classified information may be exchanged with third countries and international organisations, can be found on the Commission website.

3. The contracting authority shall ensure that contract notices for classified contracts provide information about the special security obligations related to classified information. Annex I contains a sample template for the contract notice information.

4. The contracting authority shall ensure that information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET is disclosed to tenderers only after they have signed a non-disclosure agreement, obliging tenderers to handle and protect EUCI in accordance with Decision (EU, Euratom) 2015/444 and its implementing rules.

5. All contractors which are required to handle or store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either during the performance of the classified contract itself or at the pre-contractual stage, shall hold an FSC at the required level. The following identifies the three scenarios that may arise during the tendering stage for a classified contract involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level:

- (a) no access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level during the tendering stage:

Where the contract notice or the invitation to tender concerns a contract that will involve EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level, but does not require the tenderer to handle such information at the tender stage, a tenderer which does not hold an FSC at the required level shall not be excluded from the bidding process on the grounds that they do not hold an FSC.

- (b) access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the contracting authority during the tendering stage:

Access shall be granted to tenderer personnel who hold a PSC at the required level and who have a need-to-know. Before such access is granted, the contracting authority shall verify, through the Commission security authority, with the respective NSA/DSA whether an FSC is also required under national laws and regulations at this stage.

- (c) handling or storage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the tenderer during the tendering stage:

Where the contract notice or the invitation to tender requires tenderers to handle or store EUCI on their premises, the tenderer shall hold an FSC at the required level. In such circumstances the contracting authority shall obtain, through the Commission security authority, an assurance from the relevant NSA/DSA that the tenderer has been granted an appropriate FSC. Access shall be granted to tenderer personnel who hold a PSC at the required level and who have a need-to-know.

6. In principle, an FSC shall not be required for access to RESTREINT UE/EU RESTRICTED information, either at the tender stage or for the performance of the contract. Where Member States require an FSC for contracts or subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, as listed in Annex IV, those national requirements shall not place any additional obligations on other Member States or exclude tenderers, contractors or subcontractors from Member States that have no such FSC requirements for access to RESTREINT UE/EU RESTRICTED information from related contracts/subcontracts or a competition for such. These contracts shall be performed in Member States in accordance with their national laws and regulations.

7. Where an FSC is required for the performance of a classified contract, the contracting authority shall submit, through the Commission security authority, a request to the contractor's NSA/DSA using a facility security clearance information sheet (FSCIS). Annex III, Appendix D, contains an example of an FSCIS<sup>(10)</sup>. The classified contract shall not be awarded until the contractor's NSA/DSA has confirmed the tenderer's FSC. Response to an FSCIS is provided, to the extent possible, within ten working days of the date of the request.

<sup>(10)</sup> Other forms used may differ from the example provided in these implementing rules in their design.

*Article 4***Subcontracting in classified contracts**

1. The conditions under which a contractor awarded a Commission classified contract may subcontract shall be defined in the invitation to tender and in the contract documentation. Where the classified contract permits subcontracting of some of its parts, such subcontracting shall be subject to prior written consent from the contracting authority. Before giving its consent, the contracting authority shall consult the Commission security authority.
2. Classified contracts shall be subcontracted only to economic operators registered in a Member State, or to economic operators registered in a third country or established by an international organisation where that third country or international organisation has concluded a security of information agreement with the EU or entered into an administrative arrangement with the Commission <sup>(1)</sup>.

## CHAPTER 3

**LETTING COMMISSION CLASSIFIED CONTRACTS***Article 5***Basic principles**

1. When letting a classified contract, the contracting authority, together with the Commission security authority, shall ensure that the contractor's obligations regarding the protection of EUCI provided to that contractor or generated in the performance of the contract are an integral part of the contract. Contract-specific security requirements shall take the form of a security aspects letter (SAL). A sample template of a SAL is set out in Annex III.
2. Before signing a classified contract, the contracting authority shall prepare, after consulting the Commission security authority, a security classification guide (SCG) for the tasks to be performed and information generated in the performance of the contract, or at programme or project level, where applicable. The SCG shall be part of the SAL.
3. Programme or project-specific security requirements shall take the form of a programme (or project) security instruction (PSI). The PSI may be drafted using the provisions of the SAL template as set out in Annex III. The PSI shall be developed by the Commission department managing the programme or project, in close cooperation with the Commission security authority, and submitted for advice to the Commission Security Expert Group. Where a contract is part of a programme or project with its own PSI, the SAL of the contract shall have a simplified form and shall include reference to the security provisions set out in the PSI of the programme or project.
4. The contracting authority shall be considered the originator of classified information created and handled for the performance of the contract.
5. The contracting authority, through the Commission security authority, shall notify the NSAs/DSAs of all contractors and subcontractors about the conclusion of classified contracts or subcontracts and any extensions or early terminations of such contracts or subcontracts. A list of country requirements is provided in Annex IV.
6. Contracts involving information classified RESTREINT UE/EU RESTRICTED shall include a contract security clause making the provisions set out in Annex III, Appendix E binding upon the contractor. Those contracts shall include an SAL setting out, as a minimum, the requirements for handling RESTREINT UE/EU RESTRICTED information including information assurance aspects and specific requirements to be fulfilled by the contractor under delegation from the contracting authority for the accreditation of the contractor's CIS handling RESTREINT UE/EU RESTRICTED information.

<sup>(1)</sup> The list of agreements concluded by the EU and of administrative arrangements entered into by the European Commission, under which EU classified information may be exchanged with third countries and international organisations, can be found on the Commission website.

7. Where RESTREINT UE/EU RESTRICTED information is provided to tenderers or to potential contractors, the minimum requirements mentioned in paragraph 6 shall be included in tenders or in relevant non-disclosure arrangements concluded at the tender stage.

8. Where this is required by Member States' national laws and regulations, NSAs/DSAs ensure that contractors or subcontractors under their jurisdiction comply with the applicable security provisions for the protection of RESTREINT UE/EU RESTRICTED information and conduct verification visits to contractors' facilities located in their territory. Where the NSA/DSA is not under such an obligation, the contracting authority shall ensure that the contractor implements the required security provisions set out in Annex III.

#### *Article 6*

##### **Access to EUCI by personnel of contractors and subcontractors**

1. The Commission department, as contracting authority, shall ensure that classified contracts include provisions indicating that personnel of a contractor or subcontractor who, for the performance of the classified contract or sub-contract, require access to EUCI may be granted such access only if:

- (a) it has been established that they have a need-to-know;
- (b) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, they have been granted a PSC at the relevant level by the respective NSA/DSA or any other competent security authority;
- (c) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information.

2. If a contractor or subcontractor wishes to employ a national of a non-EU country in a position that requires access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, it is the responsibility of the contractor or subcontractor to initiate the security clearance procedure of such a person in accordance with national laws and regulations applicable at the location where access to the EUCI is to be granted.

#### CHAPTER 4

##### **VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS**

#### *Article 7*

##### **Basic principles**

1. Where the Commission, contractors or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET on 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.

2. The visits referred to in paragraph 1 shall be subject to the following requirements:

- (a) the visit shall have an official purpose related to a classified contract let by the Commission;
- (b) any visitor shall hold a PSC at the required level and have a need-to-know in order to access EUCI provided or generated in the performance of a classified contract let by the Commission.

#### *Article 8*

##### **Requests for visits**

1. Visits by contractors to other contractors' facilities, or to Commission premises, that involve access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged in accordance with the following procedure:

- (a) the security officer of the facility sending the visitor shall complete all relevant parts of the request for visit (RFV) form and submit the request to the facility's NSA/DSA. A template of the RFV form is set out in Annex III, Appendix C;

- (b) the sending facility's NSA/DSA needs to confirm the visitor's PSC before submitting the RFV to the host facility's NSA/DSA (or the Commission security authority if the visit is to Commission premises);
  - (c) the security officer of the sending facility shall then obtain from its NSA/DSA the reply of the host facility's NSA/DSA (or the Commission security authority) either authorising or denying the RFV;
  - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.
2. Visits by Commission officials to contractor facilities that involve access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged in accordance with the following procedure:
- (a) the visitor shall complete all relevant parts of the RFV form and submit it to the Commission security authority;
  - (b) the Commission security authority shall confirm the PSC of the visitor before submitting the RFV to the host facility's NSA/DSA;
  - (c) the Commission security authority shall obtain a reply from the host facility's NSA/DSA either authorising or denying the RFV;
  - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.
3. An RFV may cover either a single visit or recurring visits. In the case of recurring visits, the RFV may be valid for up to one year from the start date requested.
4. The validity of any RFV shall not exceed the validity of the PSC of the visitor.
5. As a general rule, an RFV should be submitted to the host facility's competent security authority at least 15 working days before the date of the visit.

#### *Article 9*

##### **Visit procedures**

1. Before allowing visitor to have access to EUCI, the security office of the host facility shall comply with all the visit-related security procedures and rules laid down by its NSA/DSA.
2. Visitors shall prove their identity upon arrival at the host facility by presenting a valid ID card or passport. That identification information shall correspond to the information supplied in the RFV.
3. The host facility shall ensure that records are kept of all visitors, including their names, the organisation they represent, the date of expiry of the PSC, the date of the visit and the names of the persons visited. Such records shall be retained for a period of at least five years or longer if required by the national rules and regulations of the country where the host facility is located.

#### *Article 10*

##### **Visits arranged directly**

1. In the context of specific projects, the relevant NSAs/DSAs and the Commission security authority may agree on a procedure whereby visits for a specific classified contract can be arranged directly between the visitor's security officer and the security officer of the facility to be visited. A template of the form to be used for this purpose is set out in Annex III, Appendix C. Such an exceptional procedure shall be set out in the PSI or other specific arrangements. In such cases, the procedures set out in Article 8 and Article 9(1) shall not apply.

2. Visits involving access to information classified RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending and receiving entity without the need to follow the procedures set out in Article 8 and Article 9(1).

## CHAPTER 5

### TRANSMISSION AND CARRIAGE OF EUCI IN PERFORMANCE OF CLASSIFIED CONTRACTS

#### Article 11

##### Basic principles

The contracting authority shall ensure that all decisions related to EUCI transfer and carriage are in accordance with Decision (EU, Euratom) 2015/444 and its implementing rules, and with the terms of the classified contract, including the consent of the originator.

#### Article 12

##### Electronic handling

1. Electronic handling and transmission of EUCI shall be carried out in accordance with Chapters 5 and 6 of Decision (EU, Euratom) 2015/444 and its implementing rules.

The communication and information systems owned by a contractor and used to handle EUCI for the performance of the contract ('contractor CIS') shall be subject to accreditation by the responsible security accreditation authority (SAA). Any electronic transmission of EUCI shall be protected by cryptographic products approved in accordance with Article 36(4) of Decision (EU, Euratom) 2015/444. TEMPEST measures shall be implemented in accordance with Article 36(6) of that Decision.

2. The security accreditation of contractor CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the security officer of a contractor if this is permitted by national laws and regulations. Where that task is delegated, the contractor shall be responsible for implementing the minimum security requirements described in the SAL when handling RESTREINT UE/EU RESTRICTED information on its CIS. However, the relevant NSAs/DSAs and SAAs retain responsibility for the protection of RESTREINT UE/EU RESTRICTED information handled by the contractor and the right to inspect the security measures taken by the contractors. In addition, the contractor shall provide to the contracting authority and, where required by national laws and regulations, the competent national SAA, a statement of compliance certifying that the contractor CIS and related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level<sup>(12)</sup>.

#### Article 13

##### Transport by commercial couriers

The transport of EUCI by commercial couriers shall abide by the relevant provisions of Commission decisions on implementing rules for handling RESTREINT UE/EU RESTRICTED information and CONFIDENTIEL UE/EU CONFIDENTIAL information.

#### Article 14

##### Hand carriage

1. The carriage of classified information by hand shall be subject to strict security requirements.
2. RESTREINT UE/EU RESTRICTED information may be hand carried by contractor personnel within the EU, provided the following requirements are met:
  - (a) the envelope or packaging used is opaque and bears no indication of the classification of its contents;

<sup>(12)</sup> The minimum requirements for communication and information systems handling EUCI at RESTREINT UE/EU RESTRICTED level are laid down in Annex III, Appendix E.

- (b) the classified information does not leave the possession of the bearer;
- (c) the envelope or packaging is not opened *en route*.

3. For information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, hand carriage by contractor personnel within an EU Member State is arranged in advance between the sending and receiving entities. The dispatching authority or facility informs the receiving authority or facility of the details of the consignment, including reference, classification, expected time of arrival and name of courier. Such hand carriage is permitted, provided the following requirements are met:

- (a) the classified information is carried in a double envelope or packaging;
- (b) the outer envelope or packaging is secured and bears no indication of the classification of its contents, while the inner envelope bears the level of classification;
- (c) EUCI does not leave the possession of the bearer;
- (d) the envelope or packaging is not opened *en route*;
- (e) the envelope or packaging is carried in a lockable briefcase or similar approved container of such size and weight that it can be retained at all times in the personal possession of the bearer and not be consigned to a baggage hold;
- (f) the courier carries a courier certificate issued by his/her competent security authority authorising the courier to carry the classified consignment as identified.

4. For hand carriage by contractor personnel of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from one EU Member State to another, the following additional rules shall apply:

- (a) the courier shall be responsible for the safe custody of the classified material carried until it is handed over to the recipient;
- (b) in the event of a security breach, the sender's NSA/DSA may request that the authorities in the country where the breach occurred carry out an investigation, report their findings and take legal or other action as appropriate;
- (c) the courier shall have been briefed on all the security obligations to be observed during carriage and shall have signed an appropriate acknowledgement;
- (d) the instructions for the courier shall be attached to the courier certificate;
- (e) the courier shall have been provided with a description of the consignment and an itinerary;
- (f) the documents shall be returned to the issuing NSA/DSA upon completion of the journey(s) or be kept available by the recipient for monitoring purposes;
- (g) if customs, immigration authorities or border police ask to examine and inspect the consignment, they shall be permitted to open and observe sufficient parts of the consignment so as to establish that it contains no material other than that which is declared;
- (h) customs authorities should be urged to honour the official authority of the shipping documents and of the authorisation documents carried by the courier.

If a consignment is opened by customs, this should be done out of sight of unauthorised persons and in the presence of the courier where possible. The courier shall request that the consignment be repacked and shall ask the authorities conducting the inspection to reseal the consignment and confirm in writing that it was opened by them.

5. Hand carriage by contractor personnel of information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET to a third country or an international organisation will be subject to provisions of the security of information agreement or the administrative arrangement concluded between, respectively, the European Union or the Commission and that third country or international organisation.

## CHAPTER 6

**BUSINESS CONTINUITY PLANNING***Article 15***Contingency plans and recovery measures**

The Commission department, as contracting authority, shall ensure that classified contract requires the contractor to set out business contingency plans (BCP) for protecting EUCI handled in connection with the performance of the classified contract in emergency situations, and to put in place preventive and recovery measures in the context of business continuity planning to minimise the impact of incidents in relation to the handling and storage of EUCI. The contractor shall inform the contracting authority of its BCP.

*Article 16***Entry into force**

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

Done at Brussels, 17 October 2019.

*For the Commission,*  
*On behalf of the President,*  
Günther OETTINGER  
*Member of the Commission*

---

## ANNEX I

## STANDARD INFORMATION IN PROCUREMENT CONTRACT NOTICES

*(to be adapted to the contract notices used)***For contracts involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET**Other particular conditions *(if applicable)*The performance of the contract is subject to particular conditions ☒ yes ☐ no*(if yes)* Description of particular conditions:

The contract will involve access to, handling and/or storage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, which is subject to the security rules for protecting EU classified information laid down in Decision (EU, Euratom) 2015/444 and to the Decision's implementing rules <sup>(1)</sup>.

Facility security clearance will be required as well as personnel security clearances for contractor personnel handling classified information.

Special security obligations will be part of the contract (security aspects letter, annexed to the contract). Subcontracting will be subject to written prior agreement by the contracting authority and compliance with all the security rules by the subcontractor and its personnel.

**For contracts involving information classified RESTREINT UE/EU RESTRICTED**Other particular conditions *(if applicable)*The performance of the contract is subject to particular conditions ☒ yes ☐ no*(if yes)* Description of particular conditions:

The contract will involve or entail access to, handling and/or storage of information classified RESTREINT UE/EU RESTRICTED, which is subject to the security rules for protecting EU classified information laid down in Decision (EU, Euratom) 2015/444 and to the Decision's implementing rules <sup>(2)</sup>.

Special security obligations will be part of the contract (security aspects letter, annexed to the contract). Subcontracting will be subject to written prior agreement by the contracting authority and compliance with all the security rules by the subcontractor and its personnel.

---

<sup>(1)</sup> The contracting authority should insert the references once the implementing rules have been adopted.

<sup>(2)</sup> The contracting authority should insert the references once the implementing rules have been adopted.

## ANNEX II

## STANDARD PROCUREMENT CONTRACT CLAUSES

*(to be adapted to the contracts used)*

## ARTICLE XX

## SECURITY-RELATED OBLIGATIONS

**XX.1 EU classified information**

If the implementation of the contract involves using or generating EU classified information, such information must be treated in accordance with the security aspects letter (SAL) and its security classification guide (SCG) as set out in Annex 1, and Decision (EU, Euratom) 2015/444 and its implementing rules <sup>(1)</sup>, until it is declassified.

Any deliverables containing classified information must be submitted in accordance with special procedures agreed with the contracting authority.

Action tasks involving classified information must not be subcontracted without prior explicit written approval from the contracting authority.

EU classified information must not be released to any third party (including subcontractors) without prior explicit written approval from the contracting authority.

---

---

<sup>(1)</sup> The contracting authority should insert the references once the implementing rules have been adopted.

*ANNEX III*

[Annex IV (to the Framework Contract)]

**SECURITY ASPECTS LETTER (SAL)**

[Model]

---

## Appendix A

**SECURITY REQUIREMENTS**

*The contracting authority must include the following security requirements in the security aspects letter (SAL). Some clauses may not be applicable to the contract. These are shown in square brackets.*

*The list of clauses is not exhaustive. Further clauses may be added depending on the nature of the classified contract.*

**GENERAL CONDITIONS**

[N.B.: applicable to all classified contracts]

1. This security aspects letter (SAL) is an integral part of the classified contract [or subcontract] and describes contract-specific security requirements. Failure to meet these requirements may constitute sufficient grounds to terminate the contract.
2. Contractors are subject to all obligations set out in Decision (EU, Euratom) 2015/444 and its implementing rules <sup>(1)</sup>.
3. Classified information generated when performing the contract must be marked as EU classified information (EUCI) at security classification level, as determined in the security classification guide (SCG) in Appendix B to this letter. Deviation from the security classification level stipulated by the SCG is permissible only with the written authorisation of the contracting authority.
4. The rights pertaining to the originator of any EUCI created and handled for the performance of the classified contract are exercised by the Commission, as the contracting authority.
5. Without the written consent of the contracting authority, the contractor or subcontractor must not make use of any information or material furnished by the contracting authority or produced on behalf of that authority for any purpose other than that of the contract.
6. The contractor must investigate all security breaches related to EUCI and report them to the contracting authority as soon as is practicable. The contractor or subcontractor must immediately report to its responsible national security authority (NSA) or to the designated security authority (DSA), and, where national laws and regulations so permit, to the Commission security authority, all cases in which it is known or there is reason to suspect that EUCI provided or generated pursuant to the contract has been lost or disclosed to unauthorised persons.
7. After the end of the contract, the contractor or subcontractor must return any EUCI it holds to the contracting authority as soon as possible. Where practicable, the contractor or subcontractor may destroy EUCI instead of returning it. This must be done in accordance with the national laws and regulations of the country where the contractor is based, with the prior agreement of the Commission security authority, and under the latter's instruction. EUCI must be destroyed in such a way that it cannot be reconstructed, either wholly or in part.
8. Where the contractor or subcontractor is authorised to retain EUCI after termination or conclusion of the contract, the EUCI must continue to be protected in accordance with Decision (EU, Euratom) 2015/444 (hereinafter 'CD 2015/444'), and with its implementing rules <sup>(2)</sup>.
9. Any electronic handling, processing and transmission of EUCI must abide by the provisions laid down in Chapters 5 and 6 of CD 2015/444. These include, inter alia, the requirement that communication and information systems owned by the contractor and used to handle EUCI for the purpose of the contract (hereinafter 'contractor CIS') must be subject to accreditation <sup>(3)</sup>; that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 36(4) of CD 2015/444, and that TEMPEST measures must be implemented in accordance with Article 36(6) of CD 2015/444.

<sup>(1)</sup> The contracting authority should insert the references once the implementing rules have been adopted.

<sup>(2)</sup> The contracting authority should insert the references once the implementing rules have been adopted.

<sup>(3)</sup> The party undertaking the accreditation will have to provide the contracting authority with a statement of compliance, through the Commission security authority, and in coordination with the relevant national security accreditation authority (SAA).

10. The contractor or subcontractor shall have business contingency plans (BCP) to protect any EUCI handled in the performance of the classified contract in emergency situations and shall put in place preventive and recovery measures to minimise the impact of incidents associated with the handling and storage of EUCI. The contractor or subcontractor must inform the contracting authority of its BCP.

#### **CONTRACTS REQUIRING ACCESS TO INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED**

11. A personnel security clearance (PSC) is not required for compliance with the contract. However, information or material classified RESTREINT UE/EU RESTRICTED must be accessible only to contractor personnel who require such information to perform the contract (*need-to-know principle*), who have been briefed by the contractor's security officer on their responsibilities and on the consequences of any compromise or breach of security of such information, and who have acknowledged in writing the consequences of a failure to protect EUCI.
12. Except where the contracting authority has given its written consent, the contractor or subcontractor must not provide access to information or material classified RESTREINT UE/EU RESTRICTED to any entity or person other than those of its personnel who have a need-to-know.
13. The contractor or subcontractor must maintain the security classification markings of classified information generated by or provided during the performance of a contract and must not declassify information without written consent from the contracting authority.
14. Information or material classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture when not in use. When in transit, documents must be carried inside an opaque envelope. The documents must not leave the possession of the bearer and they must not be opened *en route*.
15. The contractor or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to the Commission using commercial courier companies, postal services, hand carriage or electronic means. To this end, the contractor or subcontractor must follow the programme (or project) security instruction (PSI) issued by the Commission and/or the Commission implementing rules on industrial security with regard to classified procurement contracts (\*).
16. When no longer required, documents classified RESTREINT UE/EU RESTRICTED must be destroyed in such a way that they cannot be reconstructed, either wholly or in part.
17. The security accreditation of contractor CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the security officer of a contractor if national laws and regulations so permit. Where accreditation is thus delegated, the NSAs/DSAs/SAs retain responsibility for protecting any RESTREINT UE/EU RESTRICTED information that is handled by the contractor and the right to inspect the security measures taken by the contractor. In addition, the contractor shall provide the contracting authority and, where required by national laws and regulations, the competent national SAA with a statement of compliance certifying that the contractor CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.

#### **HANDLING OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)**

18. Minimum requirements for CIS handling information classified RESTREINT UE/EU RESTRICTED are laid down in Appendix E to this SAL.

#### **CONDITIONS UNDER WHICH THE CONTRACTOR MAY SUBCONTRACT**

19. The contractor must obtain permission from the Commission department concerned, as the contracting authority, before subcontracting any part of a classified contract.

---

(\*) The contracting authority should insert the references once the implementing rules have been adopted.

20. No subcontract may be awarded to a company registered in a non-EU Member State or to an entity belonging to an international organisation, if that non-EU Member State or international organisation has not concluded a security of information agreement with the EU or an administrative arrangement with the Commission.
21. Where the contractor has let a subcontract, the security provisions of the contract shall apply *mutatis mutandis* to the subcontractor(s) and its (their) personnel. In such a case, it is the contractor's responsibility to ensure that all subcontractors apply these principles to their own subcontracting arrangements. To ensure appropriate security oversight, the contractor's and subcontractor's NSAs/DSAs shall be notified of the letting of all related classified subcontracts at the levels of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET. Where appropriate, the contractor's and subcontractor's NSAs/DSAs shall be provided with a copy of the subcontract-specific security provisions. NSAs/DSAs requiring notification about the security provisions of classified contracts at RESTREINT UE/EU RESTRICTED level are listed in the annex to the Commission's implementing rules on industrial security with regard to classified procurement contracts <sup>(1)</sup>.
22. The contractor may not release any EUCI to a subcontractor without the prior written approval of the contracting authority. If EUCI to subcontractors is to be sent frequently or as a matter of routine, then the contracting authority may give its approval for a specified length of time (e.g. 12 months) or for the duration of the subcontract.

#### VISITS

*If the standard RFV procedure is to be applied to visits involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, then the contracting authority must include paragraphs 23, 24 and 25 and delete paragraph 26. If visits involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET are arranged directly between the sending and receiving establishments, then the contracting authority must delete paragraphs 24 and 25 and include paragraph 26 only.*

23. Visits involving access or potential access to information classified RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending and receiving establishments without the need to follow the procedure described in paragraphs 24 to 26 below.
- [24. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be subject to the following procedure:
  - (a) the security officer of the facility sending the visitor shall complete all relevant parts of the RFV form (Appendix C) and submit the request to the facility's NSA/DSA;
  - (b) the sending facility's NSA/DSAs needs to confirm the visitor's PSC before submitting the RFV to the host facility's NSA/DSA (or to the Commission security authority if the visit is to Commission premises);
  - (c) the security officer of the sending facility shall then obtain from its NSA/DSA the reply of the host facility's NSA/DSA (or the Commission security authority) either authorising or denying the RFV;
  - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.]
- [25. Before giving the visitor(s) access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, the host facility must have received authorisation from its NSA/DSA.]
- [26. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged directly between the sending and receiving establishments (an example of the form that may be used for this purpose is provided in Appendix C).]

<sup>(1)</sup> The contracting authority should insert the references once the implementing rules have been adopted.

27. Visitors must prove their identity on arrival at the host facility by presenting a valid ID card or passport.
28. The facility hosting the visit must ensure that records are kept of all visitors. These must include their names, the organisation they represent, the date of expiry of the PSC (if applicable), the date of the visit and the name(s) of the person(s) visited. Without prejudice to European data-protection rules, such records are to be retained for a period of no less than five years or in accordance with national rules and regulations, as appropriate.

#### **ASSESSMENT VISITS**

29. The Commission security authority may, in cooperation with the relevant NSA/DSA, conduct visits to contractors' or subcontractors' facilities to check that the security requirements for handling EUCI are being complied with.

#### **SECURITY CLASSIFICATION GUIDE**

30. A list of all the elements in the contract which are classified or to be classified in the course of the performance of the contract, the rules for so doing and the specification of the applicable security classification levels are contained in the security classification guide (SCG). The SCG is an integral part of this contract and can be found in Appendix B to this Annex.
-

*Appendix B***SECURITY CLASSIFICATION GUIDE**

[specific text to be adjusted depending on the subject of the contract]

---

## Appendix C

**REQUEST FOR VISIT**

(MODEL)

**Detailed instructions for completion of request for visit**

(The application must be submitted in English only)

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HEADING</b>                                              | Check boxes for visit type, information type, and indicate how many sites are to be visited and the number of visitors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>4. ADMINISTRATIVE DATA</b>                               | To be completed by requesting NSA/DSA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY</b>    | Give full name and postal address.<br><br>Include city, state and post code as applicable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>6. ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED</b> | Give full name and postal address. Include city, state, post code, telex or fax number (if applicable), telephone number and email. Give the name and telephone/fax numbers and email of your main point of contact or the person with whom you have made the appointment for the visit.<br><br>Remarks:<br><br>(1) Giving the correct post code (zip code) is important because a company may have various different facilities.<br><br>(2) When applying manually, Annex 1 can be used when two or more facilities have to be visited in connection with the same subject. When an Annex is used, item 3 should state: 'SEE ANNEX 1, NUMBER OF FAC: ...' (state number of facilities). |
| <b>7. DATES OF VISIT</b>                                    | Give the actual date or period (date-to-date) of the visit in the format 'day — month — year'. Where applicable, give an alternate date or period in brackets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>8. TYPE OF INITIATIVE</b>                                | Specify whether the visit has been initiated by the requesting organisation or facility or by invitation of the facility to be visited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>9. THE VISIT RELATES TO:</b>                             | Specify the full name of the project, contract or call for tender using commonly used abbreviations only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                                                       |                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10. <b>SUBJECT TO BE DISCUSSED/JUSTIFICATION</b>                      | <p>Give a brief description of the reason(s) for the visit. Do not use unexplained abbreviations.</p> <p>Remarks:</p> <p>In the case of recurring visits this item should state 'Recurring visits' as the first words in the data element (e.g. Recurring visits to discuss_____)</p> |
| 11. <b>ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED</b> | <p>State SECRET UE/EU SECRET (S-UE/EU-S)</p> <p>or</p> <p>CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), as appropriate.</p>                                                                                                                                                            |
| 12. <b>PARTICULARS OF VISITOR</b>                                     | <p>Remark: when more than two visitors are involved in the visit, Annex 2 should be used.</p>                                                                                                                                                                                         |
| 13. <b>THE SECURITY OFFICER OF THE REQUESTING ENTITY</b>              | <p>This item requires the name, telephone number, fax number and email of the requesting facility's Security Officer.</p>                                                                                                                                                             |
| 14. <b>CERTIFICATION OF SECURITY CLEARANCE</b>                        | <p>This field is to be completed by the certifying authority.</p> <p>Notes for the certifying authority:</p> <p>(a) Give name, address, telephone number, fax number and email (can be pre-printed).</p> <p>(b) This item should be signed and stamped (if applicable).</p>           |
| 15. <b>REQUESTING SECURITY AUTHORITY</b>                              | <p>This field is to be completed by the NSA/DSA.</p> <p>Note for the NSA/DSA:</p> <p>(a) Give name, address, telephone number, fax number and email (can be pre-printed).</p> <p>(b) This item should be signed and stamped (if applicable).</p>                                      |

All fields must be completed and the form submitted via Government-to-Government channels <sup>(2)</sup>

<sup>(2)</sup> If it has been agreed that visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level can be arranged directly, the completed form can be submitted directly to the Security Officer of the establishment to be visited.



---

9. **THE VISIT RELATES TO CONTRACT:**

---

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE** *(Include details of host entity and any other relevant information. Abbreviations should be avoided):*

---

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

---

12. **PARTICULARS OF VISITOR(S)** *(Annex 2 to be completed)*

---

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

---

14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL:**

NAME:

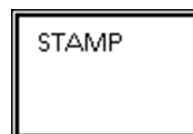
ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

DATE (dd/mm/yyyy): \_\_\_\_/\_\_\_\_/\_\_\_\_



15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:

NAME:

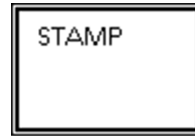
ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

DATE (dd/mm/yyyy): \_\_\_\_/\_\_\_\_/\_\_\_\_



16. **REMARKS** (Mandatory justification required in the case of an emergency visit):

<Placeholder for reference to applicable personal data legislation and link to mandatory information to the data subject, e.g. how Article 13 of the General Data Protection Regulation <sup>(3)</sup> is implemented.>

<sup>(3)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

## ANNEX 1 to RFV FORM

**ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED**

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

*(Continue as required)*

<Placeholder for reference to applicable personal data legislation and link to mandatory information to the data subject, e.g. how Article 13 of the General Data Protection Regulation <sup>(1)</sup> is implemented.>

<sup>(1)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

## ANNEX 2 to RFV FORM

**PARTICULARS OF VISITOR(S)**

1.

SURNAME:

FIRST NAMES (*as per passport*):DATE OF BIRTH (*dd/mm/yyyy*): \_\_\_\_/\_\_\_\_/\_\_\_\_

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES (*as per passport*):DATE OF BIRTH (*dd/mm/yyyy*): \_\_\_\_/\_\_\_\_/\_\_\_\_

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

*(Continue as required)*

<Placeholder for reference to applicable personal data legislation and link to mandatory information to the data subject, e.g. how Article 13 of the General Data Protection Regulation <sup>(1)</sup> is implemented.>

<sup>(1)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

## Appendix D

**FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)**

(MODEL)

**1. Introduction**

- 1.1. Attached is a sample Facility Security Clearance Information Sheet (FSCIS) for the rapid exchange of information between the National Security Authority (NSA) or Designated Security Authority (DSA), other competent national security authorities and the Commission (as contracting authority) with regard to the Facility Security Clearance (FSC) of a facility involved in classified tenders, contracts or subcontracts.
- 1.2. The FSCIS is valid only if stamped by the relevant NSA/DSA or other competent authority.
- 1.3. The FSCIS is divided into a request and reply section and can be used for the purposes identified above or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting NSA/DSA in field 7 of the request section.
- 1.4. The details contained in the FSCIS are not normally classified; accordingly, when an FSCIS is to be sent between the respective NSAs/DSAs/Commission this should preferably be done by electronic means.
- 1.5. NSAs/DSAs should make every effort to respond to an FSCIS request within ten working days.
- 1.6. Should any classified information be transferred or a contract awarded in relation to this assurance, the issuing NSA/DSA must be informed.

**Procedures and Instructions for the use of the Facility Security Clearance Information Sheet (FSCIS)**

These detailed instructions are for the NSA/DSA or the Commission contracting authority that completes the FSCIS. The request should preferably be typed in capital letters.

|                        |                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HEADER</b>          | The requester inserts full NSA/DSA and country name.                                                                                                                                                                                                                                                                                                                                           |
| <b>1. REQUEST TYPE</b> | <p>The requesting contracting authority selects the appropriate check-box for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used:</p> <p>SECRET UE/EU SECRET = S-UE/EU-S</p> <p>CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C</p> <p>CIS = Communication and information systems for processing classified information</p> |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2. <b>SUBJECT DETAILS</b>    | <p>Fields 1 to 6 are self-evident.</p> <p>In field 4 the standard two-letter country code should be used. Field 5 is optional.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 3. <b>REASON FOR REQUEST</b> | <p>Give the specific reason for the request, provide project indicators, number of contract or invitation to tender. Please specify the need for storage capability, CIS classification level, etc.</p> <p>Any deadline/expiry/award dates which may have a bearing on the completion of an FSC should be included.</p>                                                                                                                                                                                                                                                                                                                          |
| 4. <b>REQUESTING NSA/DSA</b> | <p>State the name of the actual requester (on behalf of the NSA/DSA) and the date of the request in number format (dd/mm/yyyy).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 5. <b>REPLY SECTION</b>      | <p>Fields 1-5: select appropriate fields.</p> <p>Field 2: if an FSC is in progress, it is recommended to give the requester an indication of the required processing time (if known).</p> <p>Field 6:</p> <p>(a) Although validation differs by country or even by facility, it is recommended that the expiry date of the FSC be given.</p> <p>(b) In cases where the expiry date of the FSC assurance is indefinite, this field may be crossed out.</p> <p>(c) In compliance with respective national rules and regulations, the requester or either the contractor or subcontractor is responsible for applying for a renewal of the FSC.</p> |
| 6. <b>REMARKS</b>            | <p>May be used for additional information with regard to the FSC, the facility or the foregoing items.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 7. <b>ISSUING NSA/DSA</b>    | <p>State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply in number format (dd/mm/yyyy).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)**

(MODEL)

All fields must be completed and the form communicated via Government-to-Government or Government-to-international organisation channels.

**REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE**

To: \_\_\_\_\_

(NSA/DSA Country name)

Please complete the reply boxes, where applicable:

☐ Provide an FSC assurance at the level of: ☐ S-UE/EU-S ☐ C-UE/EU-C

for the facility listed below

☐ Including safeguarding of classified material/information

☐ Including Communication and Information Systems (CIS) for processing classified information

☐ Initiate, directly or upon a corresponding request of a contractor or subcontractor, the process of obtaining an FSC up to and including the level of ..... with ..... level of safeguarding and ..... level of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.

1. Full facility name:

Corrections/Additions:

.....

.....

2. Full facility address:

.....

.....

3. Postal address (if different from 2)

.....

.....

4. Zip/post code/city/country

.....

.....

5. Name of the Security Officer

.....

.....

6. Telephone/Fax/Email of the Security Officer

.....

.....

7. This request is made for the following reason(s): (provide details of the pre-contractual (proposal selection) stage, contract or subcontract, programme/project, etc.)

Requesting NSA/DSA/Commission contracting authority: Name: ..... Date: (dd/mm/yyyy) .....

**REPLY (within ten working days)**

This is to certify that:

1. ☐ the abovementioned facility holds an FSC up to and including the level of ☐ S-UE/EU-S  
☐ C-UE/EU-C.
2. The abovementioned facility has the capability to safeguard classified information/material:  
☐ yes, level: ..... ☐ no.
3. the abovementioned facility has accredited/authorised CIS:  
☐ yes, level: ..... ☐ no.
4. ☐ in relation to the abovementioned request, the FSC process has been initiated. You will be informed when the FSC has been established or refused.
5. ☐ the abovementioned facility does not hold an FSC.
6. This FSC assurance expires on: ..... (dd/mm/yyyy), or as advised otherwise by the NSA/DSA. In the case of earlier invalidation or any changes to the information listed above, you will be informed.
7. Remarks:

Issuing NSA/DSA Name: ..... Date: (dd/mm/yyyy) .....

<Placeholder for reference to applicable personal data legislation and link to mandatory information to the data subject, e.g. how Article 13 of the General Data Protection Regulation <sup>(2)</sup> is implemented.>

<sup>(2)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

*Appendix E***Minimum requirements for protection of EUCI in electronic form at RESTREINT UE/EU RESTRICTED level handled in the contractor's CIS****General**

1. The contractor must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED information complies with the minimum security requirements as laid down in this security clause and with any other additional requirements advised by the contracting authority or, if applicable, by the national security authority (NSA) or designated security authority (DSA).
2. It is the contractor's responsibility to implement the security requirements identified in this document.
3. For the purpose of this document, a communication and information system (CIS) covers all equipment used to handle, store and transmit EUCI, including workstations, printers, copiers, fax machines, servers, network management systems, network controllers and communications controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices such as USB-sticks, CDs, SD-cards, etc.
4. Special equipment, such as cryptographic products, must be protected in accordance with its dedicated security operating procedures (SecOPs).
5. Contractors must establish a structure responsible for the security management of the CIS handling information classified RESTREINT UE/EU RESTRICTED and appoint a security officer responsible for the facility concerned.
6. The use of IT solutions (hardware, software or services) privately owned by contractor staff for storing or processing RESTREINT UE/EU RESTRICTED information is not permitted.
7. Accreditation of the contractor's CIS handling information classified RESTREINT UE/EU RESTRICTED must be approved by the security accreditation authority (SAA) of the Member State concerned or delegated to the contractor's security officer as permitted by national laws and regulations.
8. Only information classified RESTREINT UE/EU RESTRICTED that is encrypted using approved cryptographic products may be handled, stored or transmitted (by wired or wireless means) as any other unclassified information under the contract. Such cryptographic products must be approved by the EU or a Member State.
9. External facilities involved in maintenance/repair work must be contractually obliged to comply with the applicable provisions for handling of information classified RESTREINT UE/EU RESTRICTED, as set out in this document.
10. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor must provide evidence of compliance with the contract security clause. If an audit and inspection of the contractor's processes and facilities are also requested, to ensure compliance with these requirements, contractors shall permit representatives of the contracting authority, the NSA/DSA/SAA, or the relevant EU security authority to conduct such an audit and inspection.

**Physical security**

11. Areas in which CIS are used to display, store, process or transmit RESTREINT UE/EU RESTRICTED information or areas housing servers, network management systems, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be restricted to individuals with specific authorisation. Without prejudice to paragraph 8, equipment as described in paragraph 3 must be stored in such separate and controlled areas.
12. Security mechanisms and/or procedures must be implemented to regulate the introduction or connection of removable computer storage media (such as USBs, mass storage devices or CD-RWs) to components on the CIS.

**Access to CIS**

13. Access to a contractor's CIS handling EUCI is allowed on a basis of strict need-to-know and authorisation of personnel.
14. All CIS must have up-to-date lists of authorised users. All users must be authenticated at the start of each processing session.
15. Passwords, which are part of most identification and authentication security measures, must be at least nine characters long and must include numeric and 'special' characters (if permitted by the system) as well as alphabetic characters. Passwords must be changed at least every 180 days. They must be changed as soon as possible if they have been compromised or disclosed to an unauthorised person, or if such compromise or disclosure is suspected.
16. All CIS must have internal access controls to prevent unauthorised users from accessing or modifying information classified RESTREINT UE/EU RESTRICTED and from modifying system and security controls. Users are to be automatically logged off the CIS if their terminals have been inactive for some predetermined period of time, or the CIS must activate a password-protected screen saver after 15 minutes of inactivity.
17. Each user of the CIS is allocated a unique user account and ID. User accounts must be automatically locked once at least five successive incorrect login attempts have been made.
18. All users of the CIS must be made aware of their responsibilities and the procedures to be followed to protect information classified RESTREINT UE/EU RESTRICTED on the CIS. The responsibilities and procedures to be followed must be documented and acknowledged by users in writing.
19. SecOPs must be available for the users and administrators and must include descriptions of security roles and associated list of tasks, instructions and plans.

**Accounting, audit and incident response**

20. Any access to the CIS must be logged.
21. The following events must be recorded:
  - (a) all attempts to log on, whether successful or failed;
  - (b) logging off (including being timed out, where applicable);
  - (c) creation, deletion or alteration of access rights and privileges;
  - (d) creation, deletion or alteration of passwords.
22. For all of the events listed above the following information must be communicated as a minimum:
  - (a) type of event;
  - (b) user ID;
  - (c) date and time;
  - (d) device ID.
23. The accounting records should provide help to a security officer to examine the potential security incidents. They can also be used to support any legal investigations in the event of a security incident. All security records should be regularly checked to identify potential security incidents. The accounting records must be protected from unauthorised deletion or modification.
24. The contractor must have an established response strategy to deal with security incidents. Users and administrators must be instructed on how to respond to incidents, how to report them and what to do in the event of emergency.

25. The compromise or suspected compromise of information classified RESTREINT UE/EU RESTRICTED must be reported to the contracting authority. The report must contain a description of the information involved and a description of the circumstances of the compromise or suspected compromise. All users of the CIS must be made aware of how to report any actual or suspected security incident to the security officer.

#### **Networking and interconnection**

26. When a contractor CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this significantly increases the threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED information that is handled by that CIS. This includes the internet and other public or private CIS, such as other CIS owned by the contractor or subcontractor. In this case, the contractor must perform a risk assessment to identify the additional security requirements that need to be implemented as part of the security accreditation process. The contractor shall provide to the contracting authority, and where required by national laws and regulations, the competent SAA, a statement of compliance certifying that the contractor CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.
27. Remote access from other systems to LAN services (e.g. remote access to email and remote SYSTEM support) is prohibited unless special security measures are implemented and agreed by the contracting authority, and where required by national laws and regulations, approved by the competent SAA.

#### **Configuration management**

28. A detailed hardware and software configuration, as reflected in the accreditation/approval documentation (including system and network diagrams) must be available and regularly maintained.
29. The contractor's security officer must conduct configuration checks on hardware and software to ensure that no unauthorised hardware or software has been introduced.
30. Changes to the contractor CIS configuration must be assessed for their security implications and must be approved by the security officer, and where required by national laws and regulations, the SAA.
31. The system must be scanned for any security vulnerabilities at least once a quarter. Software to detect malware must be installed and kept up-to-date. If possible, such software should have a national or recognised international approval, otherwise it should be a widely accepted industry standard.
32. The contractor must develop a business continuity plan. Back-up procedures must be established to address the following:
- (a) frequency of back-ups;
  - (b) storage requirements on-site (fireproof containers) or off-site;
  - (c) control of authorised access to back-up copies.

#### **Sanitisation and destruction**

33. For CIS or data storage media that have at any time held RESTREINT UE/EU RESTRICTED information the following sanitisation must be performed to the entire system or to storage media before its disposal:
- (a) flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must be overwritten at least three times and then verified to ensure that the original content cannot be recovered, or be deleted using approved deletion software;
  - (b) magnetic media (e.g. hard disks) must be overwritten or degaussed;

- (c) optical media (e.g. CDs and DVDs) must be shredded or disintegrated;
  - (d) for any other storage media, the contracting authority or, if appropriate, the NSA/DSA/SAA should be consulted on the security requirements to be met.
34. Information classified RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to any entity that is not authorised to access information classified RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).
-

## ANNEX IV

**Facility and personnel security clearance for contractors involving RESTREINT UE/EU  
RESTRICTED information and NSAs/DSAs requiring notification of classified contracts at  
RESTREINT UE/EU RESTRICTED level <sup>(1)</sup>**

| Member State | FSC |    | Notification of contract or subcontract involving R-UE/EU-R information to NSA/DSA |    | PSC |    |
|--------------|-----|----|------------------------------------------------------------------------------------|----|-----|----|
|              | YES | NO | YES                                                                                | NO | YES | NO |
| Belgium      |     | X  |                                                                                    | X  |     | X  |
| Bulgaria     |     | X  |                                                                                    | X  |     | X  |
| Czechia      |     | X  |                                                                                    | X  |     | X  |
| Denmark      | X   |    | X                                                                                  |    | X   |    |
| Germany      |     | X  |                                                                                    | X  |     | X  |
| Estonia      | X   |    | X                                                                                  |    |     | X  |
| Ireland      |     | X  |                                                                                    | X  |     | X  |
| Greece       | X   |    |                                                                                    | X  | X   |    |
| Spain        |     | X  | X                                                                                  |    |     | X  |
| France       |     | X  |                                                                                    | X  |     | X  |
| Croatia      |     | X  | X                                                                                  |    |     | X  |
| Italy        |     | X  | X                                                                                  |    |     | X  |
| Cyprus       |     | X  | X                                                                                  |    |     | X  |
| Latvia       |     | X  |                                                                                    | X  |     | X  |

<sup>(1)</sup> These national requirements for FSC/PSC and notifications for contracts involving RESTREINT UE/EU RESTRICTED information must not place any additional obligations on other Member States or contractors under their jurisdiction.

N.B.: Notifications of contracts involving CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information are obligatory.

| Member State   | FSC                                       |    | Notification of contract or subcontract involving R-UE/EU-R information to NSA/DSA |    | PSC                                       |    |
|----------------|-------------------------------------------|----|------------------------------------------------------------------------------------|----|-------------------------------------------|----|
|                | YES                                       | NO | YES                                                                                | NO | YES                                       | NO |
| Lithuania      | X                                         |    | X                                                                                  |    |                                           | X  |
| Luxembourg     | X                                         |    | X                                                                                  |    | X                                         |    |
| Hungary        |                                           | X  |                                                                                    | X  |                                           | X  |
| Malta          |                                           | X  |                                                                                    | X  |                                           | X  |
| Netherlands    | X<br>(for defence-related contracts only) |    | X<br>(for defence-related contracts only)                                          |    |                                           | X  |
| Austria        |                                           | X  |                                                                                    | X  |                                           | X  |
| Poland         |                                           | X  |                                                                                    | X  |                                           | X  |
| Portugal       |                                           | X  |                                                                                    | X  |                                           | X  |
| Romania        |                                           | X  |                                                                                    | X  |                                           | X  |
| Slovenia       | X                                         |    | X                                                                                  |    |                                           | X  |
| Slovakia       | X                                         |    | X                                                                                  |    |                                           | X  |
| Finland        |                                           | X  |                                                                                    | X  |                                           | X  |
| Sweden         | X<br>(for defence-related contracts only) |    | X<br>(for defence-related contracts only)                                          |    | X<br>(for defence-related contracts only) |    |
| United Kingdom |                                           | X  |                                                                                    | X  |                                           | X  |

## ANNEX V

**LIST OF NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY DEPARTMENTS RESPONSIBLE FOR HANDLING PROCEDURES ASSOCIATED WITH INDUSTRIAL SECURITY****BELGIUM**

National Security Authority  
FPS Foreign Affairs  
Rue des Petits Carmes 15  
1000 Brussels  
Tel. +32 25014542 (Secretariat)  
Fax +32 25014596  
Email: nvo-ans@diplobel.fed.be

**BULGARIA**

1. State Commission on Information Security — National Security Authority  
4 Kozloduy Street  
1202 Sofia  
Tel. +359 29835775  
Fax +359 29873750  
Email: dksi@government.bg
2. Defence Information Service at the Ministry of Defence (security service)  
3 Dyakon Ignatij Street  
1092 Sofia  
Tel. +359 29227002  
Fax +359 29885211  
Email: office@iksbg.org
3. State Intelligence Agency (security service)  
12 Hajdushka Polyana Street  
1612 Sofia  
Tel. +359 29813221  
Fax +359 29862706  
Email: office@dar.bg
4. State Agency for Technical Operations (security service)  
29 Shesti Septemvri Street  
1000 Sofia  
Tel. +359 29824971  
Fax +359 29461339  
Email: dato@dato.bg

*(The competent authorities listed above conduct the vetting procedures for issuing FSCs to legal entities applying to conclude a classified contract, and PSCs to individuals implementing a classified contract for the needs of these authorities.)*

5. State Agency National Security (security service)  
45 Cherni Vrah Blvd.  
1407 Sofia  
Tel. +359 28147109  
Fax +359 29632188, +359 28147441  
Email: dans@dans.bg

*(The above security service conducts the vetting procedures for issuing FSCs and PSCs to all other legal entities and individuals in the country applying to conclude a classified contract or implementing a classified contract.)*

**CZECHIA**

National Security Authority  
Industrial Security Department  
PO BOX 49  
150 06 Praha 56  
Tel. +420 257283129  
Email: sbr@nbu.cz

**DENMARK**

1. Politiets Efterretningstjeneste  
(Danish Security Intelligence Service)  
Klausdalsbrovej 1  
2860 Søborg  
Tel. +45 33148888  
Fax +45 33430190
2. Forsvarets Efterretningstjeneste  
(Danish Defence Intelligence Service)  
Kastellet 30  
2100 Copenhagen Ø  
Tel. +45 33325566  
Fax +45 33931320

**GERMANY**

1. For matters concerning industrial security policy, FSCs, transportation plans (except for crypto/CCI):  
Federal Ministry of Economic Affairs and Energy  
Industrial Security Division — ZB3  
Villemombler Str. 76  
53123 Bonn  
Tel. +49 228996154028  
Fax +49 228996152676  
Email: dsagermany-zb3@bmwi.bund.de (office email address)
2. For standard visit requests from/to German companies:  
Federal Ministry of Economic Affairs and Energy  
Industrial Security Division – ZB2  
Villemombler Str. 76  
53123 Bonn  
Tel. +49 228996152401  
Fax +49 228996152603  
Email: zb2-international@bmwi.bund.de (office email address)
3. Transportation plans for crypto material:  
Federal Office for Information Security (BSI)  
National Distribution Agency/NDA-EU DEU  
Mainzer Str. 84  
53179 Bonn  
Tel. +49 2289995826052  
Fax +49 228991095826052  
Email: NDAEU@bsi.bund.de

**ESTONIA**

National Security Authority Department  
Estonian Foreign Intelligence Service  
Rahumäe tee 4B  
11316 Tallinn  
Tel. +372 6939211  
Fax +372 6935001  
Email: nsa@fis.gov.ee

**IRELAND**

National Security Authority Ireland  
Department of Foreign Affairs and Trade  
76-78 Harcourt Street  
Dublin 2  
D02 DX45  
Tel. +353 14082724  
Email: nsa@dfa.ie

**GREECE**

Hellenic National Defence General Staff  
E' Division (Security INTEL, CI BRANCH)  
E3 Directorate  
Industrial Security Office  
227-231 Mesogeion Avenue  
15561 Holargos, Athens  
Tel. +30 2106572022, +30 2106572178  
Fax +30 2106527612  
Email: daa.industrial@hndgs.mil.gr

**SPAIN**

Autoridad Nacional de Seguridad  
Oficina Nacional de Seguridad  
Calle Argentona 30  
28023 Madrid  
Tel. +34 913725000  
Fax +34 913725808  
Email: nsa-sp@areatec.com  
For matters concerning personnel security clearances: asip@areatec.com  
For Transportation plans and international visits: sp-ivtco@areatec.com

**FRANCE**

National Security Authority (NSA) (for policy and for implementation in fields other than the defence industry)  
Secrétariat général de la défense et de la sécurité nationale  
Sous-direction Protection du secret (SGDSN/PSD)  
51 boulevard de la Tour-Maubourg  
75700 Paris 07 SP  
Tel. +33 171758193  
Fax +33 171758200  
Email: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (for implementation in the defence industry)  
Direction Générale de l'Armement  
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)  
60 boulevard du général Martial Valin  
CS 21623  
75509 Paris Cedex 15  
Tel. +33 988670421  
Email: for forms and outgoing RFVs: dga-ssdi.ai.fct@intradef.gouv.fr  
for incoming RFVs: dga-ssdi.visit.fct@intradef.gouv.fr

**CROATIA**

Office of the National Security Council  
Croatian NSA  
Jurjevska 34  
10000 Zagreb  
Tel. +385 14681222  
Fax +385 14686049  
Email: NSACroatia@uvns.hr

**ITALY**

Presidenza del Consiglio dei Ministri  
D.I.S. - U.C.Se.  
Via di Santa Susanna 15  
00187 Roma  
Tel. +39 0661174266  
Fax +39 064885273

**CYPRUS**

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ  
Εθνική Αρχή Ασφάλειας (ΕΑΑ)  
Λεωφόρος Στροβόλου, 172-174  
Στρόβολος, 2048, Λευκωσία  
Τηλέφωνα: +357 22807569, +357 22807764  
Τηλεμοιότυπο: +357 22302351  
Email: cynsa@mod.gov.cy

Ministry of Defence  
National Security Authority (NSA)  
172-174, Strovolos Avenue  
2048 Strovolos, Nicosia  
Tel. +357 22807569, +357 22807764  
Fax +357 22302351  
Email: cynsa@mod.gov.cy

**LATVIA**

National Security Authority  
Constitution Protection Bureau of the Republic of Latvia  
P.O. Box 286  
Riga LV-1001  
Tel. +371 67025418, +371 67025463  
Fax +371 67025454  
Email: ndi@sab.gov.lv, ndi@zd.gov.lv

**LITHUANIA**

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija  
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)  
National Security Authority  
Gedimino 40/1  
LT-01110 Vilnius  
Tel. +370 70666703, +370 70666701  
Fax +370 70666700  
Email: nsa@vsd.lt

**LUXEMBOURG**

Autorité Nationale de Sécurité  
207, route d'Esch  
L-1471 Luxembourg  
Tel. +352 24782210  
Email: ans@me.etat.lu

**HUNGARY**

National Security Authority of Hungary  
H-1399 Budapest P.O. Box 710/50  
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B  
Tel. +36 13911862  
Fax +36 13911889  
Email: nbf@nbf.hu

**MALTA**

Director of Standardisation  
Designated Security Authority for Industrial Security  
Standards & Metrology Institute  
Malta Competition and Consumer Affairs Authority  
Mizzi House  
National Road  
Blata I-Bajda HMR9010  
Tel.: +356 23952000  
Fax +356 21242406  
Email: certification@mccaa.org.mt

**NETHERLANDS**

1. Ministry of the Interior and Kingdom Relations  
PO Box 20010  
2500 EA The Hague  
Tel. +31 703204400  
Fax +31 703200733  
Email: nsa-nl-industry@minbzk.nl
2. Ministry of Defence  
Industrial Security Department  
PO Box 20701  
2500 ES The Hague  
Tel. +31 704419407  
Fax +31 703459189  
Email: indussec@mindef.nl

**AUSTRIA**

1. Federal Chancellery of Austria  
Department I/12, Office for Information Security  
Ballhausplatz 2  
1014 Vienna  
Tel. +43 153115202594  
Email: isk@bka.gv.at
2. DSA in the military sphere:  
BMLVS/Abwehramt  
Postfach 2000  
1030 Vienna  
Email: abwa@bmlvs.gv.at

**POLAND**

Internal Security Agency  
Department for the Protection of Classified Information  
Rakowiecka 2A  
00-993 Warsaw  
Tel. +48 225857944  
Fax +48 225857443  
Email: nsa@abw.gov.pl

**PORTUGAL**

Gabinete Nacional de Segurança  
Serviço de Segurança Industrial  
Rua da Junqueira nº 69  
1300-342 Lisbon  
Tel. +351 213031710  
Fax +351 213031711  
Email: sind@gns.gov.pt, franco@gns.gov.pt

**ROMANIA**

Oficiul Registrului Național al Informațiilor Secrete de Stat — ORNISS  
Romanian NSA — ORNISS — National Registry Office for Classified Information  
4th Mures Street  
012275 Bucharest  
Tel. +40 212075115  
Fax +40 212245830  
Email: relatii publice@orniss.ro, nsa.romania@nsa.ro

**SLOVENIA**

Urad Vlade RS za varovanje tajnih podatkov  
Gregorčičeva 27  
1000 Ljubljana  
Tel. +386 14781390  
Fax +386 14781399  
Email: gp.uvtp@gov.si

**SLOVAKIA**

Národný bezpečnostný úrad  
(National Security Authority)  
Security Clearance Department  
Budatínska 30  
851 06 Bratislava  
Tel. +421 268691111  
Fax +421 268691700  
Email: podatelna@nbu.gov.sk

**FINLAND**

National Security Authority  
Ministry for Foreign Affairs  
P.O. Box 453  
FI-00023 Government  
Email: NSA@formin.fi

**SWEDEN**

1. National Security Authority  
Utrikesdepartementet (Ministry for Foreign Affairs)  
UD SÅK/NSA  
SE-103 39 Stockholm  
Tel. +46 84051000  
Fax +46 87231176  
Email: ud-nsa@gov.se
2. DSA  
Försvarets Materielverk (Swedish Defence Materiel Administration)  
FMV Säkerhetsskydd  
SE-115 88 Stockholm  
Tel. +46 87824000  
Fax +46 87826900  
Email: security@fmv.se

**UNITED KINGDOM**

UK National Security Authority  
Room 335, 3rd Floor  
70 Whitehall  
London  
SW1A 2AS  
Tel. +44 2072765497, +44 2072765645  
Email: UK-NSA@cabinet-office.x.gsi.gov.uk

---



