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 ([1]),

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

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 ([3]),

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 ([4]).

(7) On 4 May 2016 the Commission adopted a decision ([5]) 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,

([1]) OJ L 72, 17.3.2015, p. 41.
([2]) OJ L 72, 17.3.2015, p. 53.
([3]) OJ L 6, 11.1.2017, p. 40.
([4]) 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).
([5]) 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 ([6]) and SECRET UE/EU SECRET ([7]) 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.

([6]) 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'.

([7]) 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:

RELEASABLE TO LIECHTENSTEIN

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:

SECRET UE/EU SECRET until [dd.mm.yyyy] and **RESTREINT UE/EU RESTRICTED** thereafter

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 ([8]).

2. Pursuant to Article 19(3)(b) of Decision (EU, Euratom) 2015/444, this information may be handled in an Administrative Area ([9]), 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.

([8]) As defined in Article 18 of Decision (EU, Euratom) 2015/444.
([9]) 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 CONFIDENTIEL 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 ([10]) 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.

([10]) 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