Official Journal
of the European Union

EN
L series

2024/1418

24.5.2024

Delegated Decision No 19/2024 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information

THE ADMINISTRATIVE COMMITTEE OF THE EUROPEAN COURT OF AUDITORS,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 287 thereof;

Having regard to Decision No 41/2021 of the Court of Auditors on the security rules for protecting EU classified information (EUCI) ([1]), hereafter "Decision No 41/2021";

Having regard to the Court of Auditors' information security policy (currently DEC 127/15 FINAL) and information classification policy (Staff Notice No 123/20) ([2]);

Having regard to the Administrative Committee's discussions at its meeting of 18 March 2024;

Whereas Decision No 41/2021 applies to all the departments and premises of the Court of Auditors;

Whereas Article 1(3) of Decision No 41/2021 provides that arrangements shall be made so that Court of Auditors staff who need to access higher levels of EUCI can do so in suitable premises of other EU institutions, bodies or agencies;

Whereas Articles 1(3) and 5(6) of Decision No 41/2021 provides that the Court of Auditors may conclude a service level agreement with another EU institution in Luxembourg in order to be able to handle and store information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above in a Secured Area of that institution, and a Memorandum of Understanding was signed with the Commission Directorate-General for Human Resources and Security on 25/09/2023 on use of the security directorate's secured area in Luxembourg;

Whereas security measures for protecting EU classified information (EUCI) throughout its life-cycle are to be commensurate in particular with its security classification;

Whereas security measures to protect the confidentiality, integrity and availability of information communicated to the Court of Auditors must be appropriate for the nature and type of information concerned;

Whereas Article 3(3) of Decision No 41/2021 requires all EUCI to be protected by physical security measures, and information classified as CONFIDENTIEL EU/CONFIDENTIAL EU or above shall additionally be protected by personnel security measures;

Whereas Article 10(10) of Decision No 41/2021 provides that the Administrative Committee shall adopt a delegated decision laying down implementing rules; pursuant to Articles 8(1) and 10(1) of Decision No 41/2021, these shall concern matters such as handling and storing EUCI as well as breaches of security;

Whereas the Court of Auditors ensured through Decision No 41/2021 that its security measures to guarantee a high level of protection for EUCI are equivalent to those established by the rules on the protection of EUCI adopted by the other EU institutions, agencies and bodies;

Whereas a lightweight administrative agreement between the Court of Auditors and the Commission, the Council and the EEAS entered into force on 27 January 2023;

([1]) OJ L 256, 19.7.2021, p. 106.
([2]) Available at https://www.eca.europa.eu/en/legal-framework.

HAS DECIDED:

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 ([3]) and SECRET UE/EU SECRET ([4]) level in compliance with Decision No 41/2021 of the Court of Auditors.

2. This Decision shall apply to all the departments and the premises of the Court of Auditors. It also applies to its Chambers and Committees, which are included in the term "departments" for the purposes of this Decision.

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 Court of Auditors 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, in writing, their responsibilities for protecting the information concerned; and

(d) the individual has obtained security clearance and been granted authorisation for access by the Director of Human Resources, Finance and General Services of the Court of Auditors up to the relevant level and until a specified date, in accordance with Article 4(4) of Decision No 41/2021.

2. Court of Auditors 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.

([3]) Pursuant to Article 1(2)(a) of Decision No 41/2021, CONFIDENTIEL UE/EU CONFIDENTIAL information means "information and material whose unauthorised disclosure could harm the essential interests of the European Union or of one or more of the Member States".

([4]) Pursuant to Article 1(2)(a) of Decision No 41/2021, SECRET UE/EU SECRET information means "information and material whose unauthorised disclosure could seriously harm the essential interests of the European Union or of one or more of the Member States".

CHAPTER 2

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

Article 3

Originator

While the originator within the meaning of Article 2(m) of Decision No 41/2021 is the EU 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.

Article 4

Assigning a classification level

1. 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.

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

(a) create international tension;

(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.

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 CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level 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, following confirmation from the originator of the document that it is safe to do so.

Article 6

Record of source material

To allow the exercise of originator control in accordance with Article 14 below, originators of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents shall keep a record of all 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 point 12 of the Court of Auditors' information classification policy, the overall classification level of a document shall be at least 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 means of a classification marking, if the information is delivered in written form (whether on paper, on removable storage media or in a Communication and Information System (CIS)), or through an announcement if the information is delivered in oral form (e.g. a conversation or presentation). Classified material shall be physically marked 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 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 placed 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 on 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 all sides.

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 annexes and enclosures shall be listed, whenever possible on the first page; and

(e) the date of creation shall be indicated on the document.

5. Where possible, the SECRET UE/EU SECRET marking shall appear in red.

Article 9

Abbreviated C-UE/EU-C and S-EU/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 of, respectively, a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET document, or where the full classification marking cannot be placed, for example on a small removable storage medium. It may be used in the body of text where the repeated use of full classification markings would be 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. For example:

RELEASABLE TO LIECHTENSTEIN

2. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents may bear a security caveat with specific instructions for handling and managing the documents.

Whenever possible, any indications for declassifying shall be given 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, Court of Auditors staff shall use a CIS accredited for at least the corresponding classification level. In case of doubt, advice should be sought from the Information Security Officer of the Court of Auditors (hereafter "ISO").

3. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents, including drafts (see Article 5), must 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, may be used to print 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 the Secured Area of the Commission in Luxembourg for the use of which the Court of Auditors has concluded a Memorandum of Understanding; and

— when it arrives in or leaves a CIS.

2. The information may be registered on paper or in electronic logbooks.

3. If the information is handled electronically in a CIS, registration may also be covered by processes within the CIS itself. In this event, the CIS must include measures to guarantee the integrity of records.

4. The Registry Control Officer shall keep a register with 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 to create 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 to whom to distribute the information, based on their need-to-know. A distribution list shall be drawn up to ensure the need-to-know principle is correctly enforced.

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; or

(d) disclosed to a party outside the Court of Auditors but within the EU.

2. Holders of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information are duly authorised individuals who 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 such information in accordance with Decision No 41/2021. Unlike originators of classified information, holders are not 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 Court of Auditors department holding the classified information shall exercise originator control. If the holder considers it necessary to release CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information to a third country or international organisation, the Court of Auditors shall seek advice from one of the parties to a Security of Information Agreement with that same third country or international organisation ([5]).

Article 15

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

CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be handled and transmitted electronically if possible. In line with Article 6 of Decision No 41/2021, only CIS and equipment that have been accredited by another EU institution, agency or body, or by the Court of Auditors, may be used for this purpose.

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, such as USB sticks, CDs, DVDs or memory cards (including SSDs ([6])), shall be strictly controlled and accounted for. Only removable storage media provided by the Court of Auditors or by another EU institution, body or agency and approved by the ISO, and encrypted by a product approved by the ISO, may be used. Personal removable storage media and those distributed freely at conferences, seminars, etc. must not be used to transfer classified information. In line with ISO guidance, Tempest-proof removable storage media should be used where possible.

([5]) See Article 35 for further details.

([6]) SSD means semiconductor storage device, solid-state device or solid-state disk.

2. Where a classified document is handled or stored electronically on a removable storage media, the classification marking shall be clearly displayed as part of the 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 devices may warrant a higher classification level.

4. Only properly accredited CIS may be used to transfer CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information to or from removable storage media.

5. Before downloading such information to a removable storage media, particular care shall be taken to ensure that the media does not contain viruses or malware.

6. Where applicable, removable storage media shall be handled in accordance with security operating procedures relating to the encryption system used.

7. Documents on removable storage media that are either no longer required, or that have been transferred to 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 be done in accordance with the Court of Auditors' security rules. An inventory shall be kept of removable storage 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 5(5) and (6) of Decision No 41/2021, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be handled in a Secured Area ([7]). Such information may also be accessed by Court of Auditors staff in Secured Areas of another EU institution.

2. Pursuant to Article 5(6) of Decision No 41/2021, and if specifically agreed by the originator, this information may exceptionally be handled in the Administrative Area ([8]) of the Court of Auditors, provided the EUCI is protected from access by unauthorised persons.

3. In times of crisis or in the event of an emergency, this information may be handled outside a Secured or Administrative Area, provided the holder has undertaken to apply compensatory measures 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 holder's personal control.

— In the case of documents in paper form, the holder has notified the Registry for EUCI, as soon as possible and depending on the nature of the crisis or emergency situation, that the classified documents are being handled outside a Secured or Administrative Area.

— Documents shall be stored in an appropriate safe when they are not being read or discussed.

— The doors to the room shall be closed while documents are being read or discussed.

— Document details may not be discussed over a non-secure phone line or by email.

— The holder shall not photocopy or scan documents. Only the Registry for EUCI may provide additional copies.

([7]) As defined in Article 18 of Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

([8]) As defined in the Annex to Decision No 41/2021.

— Documents may only be handled and temporarily held outside an Administrative or Secured Area for as long as is absolutely necessary, after which they shall be returned to the Registry for EUCI.

— On return, documents shall be signed for.

— The holder must neither throw classified documents away nor destroy them.

4. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information shall be stored in a Secured Area, in either a security container or a strong room.

5. Further advice can be sought from the ISO.

6. Any suspected or actual security incidents involving a document shall be reported to the ISO 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 specifically agreed and not imposed any caveats. However, no more copies shall be made than are strictly necessary. The Court of Auditors may also ask the originator to provide a copy translated into English.

2. Where only part of a classified document is reproduced, the same conditions as are applicable to copies of the entire document shall apply. 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 apply 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 a Secured Area, or an Administrative Areas in compliance with article 17(2), shall be sent electronically by appropriately accredited means and/or protected by approved cryptographic products.

2. Depending on the available means and the particular circumstances, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be physically carried by hand in paper form 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. In accordance with Article 6(8) of Decision No 41/2021, the removable storage media shall be encrypted by means of a product approved for the protection of EUCI, either by the Council, or by the Secretary-General of the Council, in its function as crypto approval authority, or by another EU institution, agency or body. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information on removable storage media that are not protected by an encryption product approved in this way shall be handled in the same manner as information in paper form.

4. Consignments 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 hidden 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 be sealed and must not give any indication of the nature or classification level of the contents. The inner layer of packaging shall be marked 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 issued with a courier certificate.

7. Envelopes and packages must not be opened en route. The security authorisation given to the courier does not entitle them to access the classified information in the consignment.

8. Under Article 5(12) of Decision No 41/2021, the originator may also impose additional physical security measures to protect the information against unauthorised disclosure during transport.

9. Any suspected or actual security incidents involving CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information that is carried by staff or couriers shall be reported to the ISO for subsequent investigation as soon as possible.

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 giving details of the removable storage media and all the files they contain, so that the recipient can make the necessary verifications and confirm receipt.

2. The devices shall store only the EUCI being transported. All the classified information on a single device must be intended for the same recipient. Senders should bear in mind that large amounts of classified information stored on the same device 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. All CONFIDENTIEL UE/EU CONFIDENTIAL and 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 departments and on Court of Auditors premises

1. Security authorised staff may carry CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents within departments and on Court of Auditors premises, but the documents must not leave the bearer's possession 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 European Union

1. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information may be carried by staff or couriers of the Court of Auditors, or of the originating EU institution, body or agency, 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 outer packaging shall be sealed and shall not give any indication of the nature or classification level of its contents.

(b) The CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information must not leave the bearer's possession.

(c) The envelope or packaging must not be opened en route, and the information must not be read in public.

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:

(a) national postal services that track consignments, or commercial courier services that guarantee personal hand carriage, provided they meet the requirements set out in Article 24 of this Decision;

(b) military, government or diplomatic courier, in coordination with Records Office staff.

3. Staff wishing to send SECRET UE/EU SECRET information to other EU Member States may only arrange with the Registry Control Officer for it to be conveyed by military, government or diplomatic courier, not by a postal service or commercial courier.

4. All Court of Auditors staff or official couriers bearing CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall carry a courier certificate for each consignment. The certificate shall be issued by the Registry Control Officer and state 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 of the Court of Auditors, or of the originating EU institution, body or agency, 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 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 shall be 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 checks.

— The bearer shall carry a courier certificate issued by the Registry Control Officer and stating that they are authorised to carry the CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignment.

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 an EU Member State or between two Member States. Commercial couriers may convey SECRET UE/EU SECRET information within a Member State, but not abroad.

3. Commercial courier services shall be instructed that they must deliver CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignments only to the Registry Control Officer, their duly authorised substitute or 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.

Article 25

Preparation of EUCI for transport by commercial courier services

1. When preparing classified consignments, senders shall bear in mind that commercial courier services may only deliver CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET consignments to the Registry Control Officer, their duly authorised substitute, or the intended recipient.

2. Consignments of information sent through an approved commercial courier service shall be prepared and packaged as follows:

(a) The information shall be placed in an opaque double envelope (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 marked on the inner envelope or layer of packaging.

(c) The outer packaging shall be sealed and shall not bear any classification marking.

(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 state 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, not itself classified, shall quote the reference number, date and copy number of the document, but must not state the subject matter.

(f) The outer envelope or packaging must contain a delivery receipt. The delivery receipt, which itself shall not be classified, shall quote the reference number, date and copy number of the document, but must not state the subject matter.

(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. Before sending a consignment, the sender shall agree a suitable date and time for delivery with the named recipient.

4. The sender shall bear sole responsibility for any consignment sent through a commercial courier service. In the event that a consignment is lost or not delivered on time, the sender shall inform the ISO and the Registry Control Officer, who will follow up the security incident.

Article 26

Other specific handling conditions

1. Any additional carriage conditions set out in a security of information agreement or administrative arrangements shall be complied with. If in doubt, staff should consult the ISO or the Registry Control Officer.

2. The double packaging requirement can be waived for classified information that is protected by approved cryptographic products. However, for addressing purposes, and because removable storage media bear an explicit security classification marking, they shall be carried in at least a sealed opaque envelope with, where appropriate, additional physical protection measures, such as a bubble-wrap envelope.

CHAPTER 4

CLASSIFIED MEETINGS

Article 27

Preparing for a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting

1. Meetings at which CONFIDENTIEL UE/EU CONFIDENTIEL or SECRET UE/EU SECRET information is to be discussed shall only be held in a meeting room that has been accredited at the appropriate level or above. The Court of Auditors may use meeting rooms in the Secured Area of another EU institution. Where these are not available, staff shall seek the advice of the ISO.

2. As a general rule, meeting agendas should not be 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 interests of the Union or any Member States.

3. Meeting organisers shall remind participants that any comments submitted on a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET agenda item must not be sent by email or any other means that has not been duly 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 have been duly authorised, may be present during discussion of classified items.

5. Meeting invitations must give advance warning that the agenda will include classified topics, and that appropriate security measures will apply.

6. Meeting organisers shall remind participants 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 in advance. In accordance with Article 4(6) of Decision No 41/2021, they shall also inform the ISO in good time of the meeting dates, times, venues and lists of participants.

Article 28

Participant access to a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting

1. Meeting organisers shall inform the ISO and the Registry Control Officer of any external visitors who will be attending a CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting organised by the Court of Auditors.

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 CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET meeting rooms

Only IT systems accredited in accordance with Article 11 of this Decision may be used where CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information is conveyed, for example in the course of a presentation or videoconference.

Article 30

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

1. At the start of a classified discussion, the chair shall announce to the meeting that it is moving to 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 all documents used by the interpreters, shall be signed for and returned to the Registry Control Officer for destruction in approved shredders ([9]).

5. A note shall be taken during the meeting of the list of participants, together with an outline of any classified information shared with Member States and released orally to third countries or international organisations, for inclusion 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 ([10]), or who have a contractual link to the Court of Auditors or another EU institution, shall have access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information.

([9]) See Article 42(6) for further details.

([10]) Regulation No 31 (EEC) laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants, as amended (OJ 45, 14.6.1962, p. 1385/62) (ELI: http://data.europa.eu/eli/reg/1962/31(1)/2023-01-01).

CHAPTER 5

SHARING AND EXCHANGING CONFIDENTIEL UE/EU CONFIDENTIAL AND SECRET UE/EU SECRET INFORMATION

Article 32

Originator consent

If the Court of Auditors is not the originator of the classified information for which release or sharing is desired, or of the source material it may contain, the Court of Auditors department which holds the classified information shall first seek the originator's written consent to release. If the originator cannot be identified, the Court of Auditors department holding the 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 may only be shared with another EU institution, agency, body or office if the recipient has a need-to-know and the entity has a corresponding legal arrangement with the Court of Auditors.

2. Within the Court of Auditors, the Registry for EUCI shall, as a general rule, be the main point of entry and exit for classified information exchanges with other EU institutions, agencies, bodies and offices.

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 obtained security clearance.

2. Member States' classified information that bears an equivalent national classification marking [11] and has been provided to the Court of Auditors 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 put an appropriate legal or administrative framework in place, such as a security of information agreement or an administrative arrangement with the Court of Auditors. The provisions of any such agreement or arrangement shall prevail over those of this Decision.

2. The Registry for EUCI shall, as a general rule, be the main point of entry and exit for all CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information exchanged between the Court of Auditors and third countries or international organisations.

[11] The table of equivalence for Member State markings is set out in Annex I to Decision (EU, Euratom) 2015/444.

3. All classified information received from a third country or an international organisation shall be registered for security purposes. Staff shall therefore contact the Registry for EUCI 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 the Secured Area; and

— when it arrives in or leaves a CIS.

5. The information may be registered on paper or in electronic logbooks.

6. Registration procedures for handling classified information 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 a third country or an international organisation shall be afforded an equivalent level of protection as the EUCI bearing an equivalent classification marking in accordance with the relevant 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 Court of Auditors 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 EU entity, but no security of information agreement or administrative arrangement is in place, the exceptional ad hoc release procedure shall be applied.

2. Court of Auditors departments shall contact the ISO and the originator. The Court of Auditors shall seek advice from one of the Parties to a Security of Information Agreement with that same third country, international organisation or EU entity.

3. After this consultation, the College of the Court of Auditors may, on the basis of a proposal by the Secretary-General, 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 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 to determine whether the original classification level is still appropriate.

2. Court of Auditors 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 Court of Auditors department that created a classified document shall be responsible for deciding whether it can be downgraded or declassified. At the Court of Auditors, all requests for downgrading and declassifying shall be subject to consultation of the Head of Department or Director of the originating department, or the head of task. 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 Court of Auditors department no longer exists and its responsibilities have been transferred to another department, the decision on downgrading or declassifying lies with this department. Where the originating department no longer exists and its responsibilities have not been transferred, the decision to downgrade or declassify shall be taken jointly by the directors of the Court of Auditors.

4. The department responsible for downgrading or declassifying shall work with the Registry for EUCI on the practical arrangements for downgrading or declassification.

Article 39

Sensitive non-classified information

When reviewing a document results in a decision to declassify, consideration shall be given to marking the document as sensitive non-classified information within the meaning of point 16 of the Court of Auditors information classification policy ([12]) and point 4 of the Guidelines on classifying and handling non-EU-classified information.

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" function 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 Court of Auditors' Archives Service shall be notified of all declassification decisions.

5. All translations of classified information shall be subject to the same downgrading or declassification procedures as the original language version.

([12]) Available at: https://www.eca.europa.eu/en/legal-framework.

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. Partial declassification of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information shall result in production of a declassified extract.

3. In the declassified extract, parts that remain classified shall be replaced by:

PART NOT TO BE DECLASSIFIED

either in the body of the text, if the part that remains classified is a part of a paragraph, or as a paragraph, if the part that remains classified runs to one or more complete paragraphs.

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 Court of Auditors shall not amass large quantities of classified information.

2. Originating departments shall review documents at least every 5 years for destruction or deletion. This shall apply both to information in paper form and to information stored in a 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 the 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 to destroy 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 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 working life. Electronic data shall be destroyed or erased from IT resources and associated storage media in a manner that gives reasonable assurance that the information cannot be recovered. Sanitisation shall entail removing all data from the storage devices, as well as all labels, markings and activity logs.

10. Computer storage media shall be given to the ISO for destruction and disposal after the Registry Control Officer has been informed.

Article 43

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

1. In accordance with the Memorandum of Understanding between the Court of Auditors and the Commission's Directorate General for Human Resources and Security on the use of its Secured Area, the established Commission emergency procedure for safeguarding classified information shall apply. If necessary, the Commission's DS Lux Local Security Officer will have access to the Court of Auditors' safe in order to apply the established Commission emergency procedure and activate any 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:

(i) moving EUCI to an alternative safe place, where possible a Secured Area within the same building;

(ii) evacuating EUCI to an alternative safe place, where possible a Secured Area in a different building, preferably of an EU institution;

(iii) destroying EUCI, where possible using an approved means of destruction.

2. If 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 information thereafter.

3. The operational details of emergency evacuation and destruction plans shall themselves be classified RESTREINT UE/EU RESTRICTED. A copy shall be kept in each safe that is used to store 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 Court of Auditors' information security policy, information classification policy and archives policy.

2. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents must 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 Court of Auditors staff and all other individuals to whom it applies, and shall be published in the Official Journal of the European Union.

Article 46

Entry into force

After adoption by the Administrative Committee, this Decision shall enter into force on the day following that of its publication in the Official Journal of the European Union.

Done at Luxembourg, 19 March 2024.

For the Administrative Committee of the Court of Auditors
The President
Tony MURPHY

ANNEX

Categories of staff who may have access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information where necessary in order to perform their duties

Categories of Court of Auditors personnel	Access to CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET information	Conditions
Members	yes	briefing + acknowledge
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 from EU Member States	yes	Only if cleared by the originating Member States prior to taking up their assignment + briefed by the Court of Auditors + acknowledge + authorised by the Court of Auditors + need-to-know
Trainees	no	No exceptions possible
Any other category of staff (interim, intra-muros externals, etc.)	no	No exceptions possible