EUROPEAN
COURT
OF AUDITORS

Decision № 41-2021 of the Court of Auditors on the security rules for protecting EU classified information (EUCI)

THE EUROPEAN COURT OF AUDITORS,

HAVING REGARD TO Article 13 of the Treaty on European Union,

HAVING REGARD TO Article 287 of the Treaty on the Functioning of the European Union,

HAVING REGARD TO Article 257 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union,

HAVING REGARD TO Article 1(6) of the rules for implementing the Rules of Procedure of the Court of Auditors (Decision No 21-2021 of the Court of Auditors),

HAVING REGARD TO the security rules for protecting EU classified information of the other EU institutions, agencies and bodies,

HAVING REGARD TO the Court of Auditors' information security policy (DEC 127/15 FINAL) and information classification policy (Staff Notice 123/2020),

WHEREAS pursuant to Article 287(3) TFEU, the Court of Auditors has the right of access to all relevant documents and information necessary, in its view, to carry out its mandate, including EU classified information (EUCI), which is to be carried out in full compliance with the principle of sincere cooperation among the institutions and the principle of conferral; that right of access to EUCI, guaranteed by the TFEU, cannot be called into question by the originator of EUCI, whereas the Court of Auditors may be asked to put in place and respect certain security measures, as further detailed herein;

WHEREAS the Members of the Court of Auditors, and its officials and other staff, are bound, even after leaving the service, by an obligation of confidentiality under Article 339 TFEU, Article 17 of the Staff Regulations and acts adopted pursuant thereto;

WHEREAS given its sensitive nature, the handling of EUCI requires compliance with the obligation of confidentiality to be ensured by means of appropriate security measures that can guarantee a high level of protection for that information and which are equivalent to those established by the rules on the protection of EUCI adopted by the other EU institutions, agencies and bodies, it being understood that, in the event the Court of Auditors considers that any such security measures are not justified in light of the nature and type of EUCI, the

Court of Auditors reserves its right to raise any observations it deems appropriate, while respecting the classification level of EUCI;

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 access to classified information must be provided to the Court of Auditors in accordance with the need-to-know principle for the purpose of carrying out the tasks entrusted by the Treaties and by legal acts adopted on the basis of the Treaties;

WHEREAS given the nature and sensitive content of certain information, it is appropriate to establish a special procedure for the handling by the Court of Auditors of documents containing EUCI;

WHEREAS the institution must ensure that this Decision is implemented in accordance with all applicable rules, in particular the provisions on the protection of personal data, the physical security of persons, buildings and IT, and public access to documents;

HAS DECIDED:

Article 1. Subject matter and scope

1. This Decision lays down the basic principles and minimum security standards for the protection of classified information handled by the Court of Auditors in the exercise of its mandate.

2. For the purposes of this Decision, classified information shall mean any or all of the following types of information:

   a) 'EU classified information' (EUCI) as defined in the security rules of other EU institutions, agencies, bodies or offices, and which bears one of the following security classification markings:

   - TRÈS SECRET UE/EU TOP SECRET: information and material whose unauthorised disclosure could cause exceptionally serious damage to the essential interests of the European Union or of one or more of the Member States;
   - SECRET UE/EU SECRET: 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;
   - CONFIDENTIEL UE/EU CONFIDENTIAL: information and material whose unauthorised disclosure could harm the essential interests of the European Union or of one or more of the Member States;
   - RESTREINT UE/EU RESTRICTED: information and material whose unauthorised disclosure could be disadvantageous to the interests of the European Union or of one or more of the Member States.

   b) classified information provided by Member States and bearing a national security classification marking equivalent to one of the EUCI security classification markings[1] listed in point (a);

[1] See Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union of 4 May 2011 and its Annex (OJ 2011/C 202/13).

c) classified information provided to the European Court of Auditors by third States or international organisations and bearing a security classification marking equivalent to one of the EUCI security classification markings listed in point (a), in accordance with the relevant security of information agreements or administrative arrangements.

3. The Court of Auditors shall handle RESTREINT UE/EU RESTRICTED level information on its premises and take all the necessary protective measures to this end. Arrangements shall be made for Court of Auditors staff who need to access higher levels of EUCI to do so in suitable premises of other EU institutions, bodies or agencies.

4. This Decision shall apply to all the departments and the premises of the Court of Auditors.

5. Save where a provision concerns specific groups of staff, this Decision shall apply to the Members of the Court of Auditors, the staff of the Court of Auditors who are covered by the Staff Regulations and the Conditions of Employment of Other Servants of the European Union[2], national experts seconded to the Court of Auditors (SNEs), service providers and their staff, trainees and any persons with access to the buildings and other properties of the Court of Auditors, or to information managed by the Court of Auditors.

6. Unless otherwise specified, the provisions on EUCI shall apply in an equivalent way to the classified information referred to in paragraph 2(b) and (c) of this Article.

Article 2. **Definitions**

For the purposes of this Decision:

a) 'authorisation for access to EUCI' means a decision taken by the Director of Human Resources, Finance and General Services of the Court of Auditors on the basis of assurance given by a competent authority of a Member State that a Court of Auditors official, other member of staff or SNE may be authorised, provided their need to know has been established and they have been properly informed of their responsibilities, to have access to EUCI up to a given classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) and until a given date; the individual in question will then be 'security authorised';

b) 'classification' means the assignment of a classification level to information based on the degree of prejudice which could be caused by its unauthorised disclosure;

c) 'cryptographic material' means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation, as well as keying material;

d) 'declassification' means the removal of any security classification;

e) 'document' means any recorded information, whatever its form or physical characteristics;

f) 'downgrading' means a reduction in the level of security classification;

g) 'Facility Security Clearance' means an administrative determination by a competent security authority that, from the security viewpoint, a facility can afford an adequate level of protection for EUCI at a given security classification level;

h) 'handling' of EUCI means all possible actions to which EUCI may be subject throughout its life: creation, registration, processing, carriage, downgrading, declassification and destruction. In relation to Communication and Information Systems (CIS) it also comprises its collection, display, transmission and storage;

[2] Regulation No 31 (EEC) laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants, as amended, OJ 01962R0031-01.01.2020-019.003-1 (https://eur-lex.europa.eu/eli/reg/1962/31(1)/2020-01-01).

i) ‘holder’ means a duly authorised individual with an established need-to-know who is in possession of classified information and, therefore, responsible for protecting it;

j) ‘information security authority’ means the Court of Auditors’ information security officer, who may delegate, in whole or in part, the tasks provided for in this Decision;

k) ‘information’ means any written or oral information, whatever the medium or author;

l) ‘material’ means any medium, data carrier or item of machinery or equipment;

m) ‘originator’ means an EU institution, body or agency, a Member State, a third State or an international organisation under whose authority information was created and/or introduced into EU structures;

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

o) ‘Personnel Security Clearance Certificate’ (PSCC) means a certificate issued by the Director of Human Resources, Finance and General Services of the Court of Auditors establishing that an individual holds a valid security clearance or a security authorisation and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the period of validity of that security clearance or authorisation and the expiry date of the certificate itself;

p) ‘physical security authority’ means the Head of Security of the Court of Auditors, who shall be responsible for implementing the necessary physical security measures and procedures to protect EUCI;

q) ‘Records Office’ shall be administered by the Secretariat of the Court, located in an Administrative Area under the responsibility of the Court of Auditors’ Director of Human Resources, Finance and General Services. It is responsible for the entry and exit of RESTREINT UE/EU RESTRICTED information, or its equivalent, exchanged with the Court of Auditors.

r) ‘Registry for EUCI’ shall be an area established inside a Secured Area. This Registry shall be managed by the Court of Auditors’ security-cleared and authorised Registry Control Officer. It is responsible for the entry and exit of CONFIDENTIEL UE/EU CONFIDENTIAL information or above, or its equivalent, exchanged with the Court of Auditors.

s) ‘Security Accreditation Authority (SAA)’ means the Director of Human Resources, Finance and General Services of the Court of Auditors.

Article 3. **Measures for protecting EUCI**

1. The Court of Auditors shall ensure the protection of all classified information provided to it in a manner commensurate with the classification level determined by the originator, and in accordance with this Decision.

2. To that end, the Court of Auditors shall make the handling of EUCI subject to physical and, where appropriate personnel security measures, including access authorisations for the identified persons and measures for the protection of communication and information systems. These measures are described in Articles 4 to 6 and shall apply throughout the life-cycle of the EUCI. They shall be commensurate to the EUCI’s security classification, the form and volume of information or material, the location and construction of the establishments

where the EUCI is held, and the locally assessed threat of malicious and/or criminal activity, including espionage, sabotage and terrorism.

3. EUCI shall be protected by physical security measures, and information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above shall additionally be protected by personnel security measures.

4. EUCI may only be provided to persons with a need to know within the institution. The holder of any item of EUCI must protect it as required by this Decision.

5. EUCI must not be disclosed orally or in writing. The Court of Auditors' preliminary observations, reports, opinions, press releases and other products, its website and intranet, oral interventions, replies to document access requests[3] and voice or video recordings must not contain or refer to EUCI or extracts thereof. However, if the originator has published documents or information containing a reference to EUCI, that reference may be mentioned.

6. Notwithstanding paragraph 5, the Court of Auditors and the originator may agree that, in the case of a specific audit, the Court of Auditors may reproduce or use elements of EUCI in a document. In such an event, that Court of Auditors document shall be first addressed to the originator of the EUCI in question before or during the adversarial procedure. In this situation, the Court of Auditors and the originator shall agree on whether to classify the document issued by the Court of Auditors. Where a reporting Member of the Court of Auditors deems it necessary to communicate an audit report that has been classified in whole or in part to certain addressees at the European Parliament or the Council – account being taken of all the security measures associated with this Decision – this shall require consent from the originator of the classified information. The legal framework and procedure for the exchange of such documents is set out in Article 7.

7. Where the exercise of its mandate requires certain elements of a classified document or information to be shared more widely, the Court of Auditors shall, by taking duly into account the security classification marking, consult the originator, before deciding to use those elements or information, if it deems there is an overriding public interest in doing so. The information shall only be used in the report in such a way that the interest of the originator cannot be harmed. This could be safeguarded in an appropriate manner by asking the originator to provide comments for reaching agreement on the way to anonymise, condense or generalise the information, etc. and at the same time respect the interests of those primarily concerned by the published information.

8. The Court of Auditors shall not provide EUCI to another EU institution, agency, body or office, a Member State, a third State or an international organisation without the originator's prior consultation and express written consent.

9. Unless the originator of a document classified as SECRET UE / EU SECRET or below has imposed restrictions on its duplication or translation, such documents may be duplicated or translated at the holder's request and in compliance with the practical work instructions of the information security authority at the Court of Auditors. The security measures applicable to the original document shall also apply to copies and translations thereof.

10. If the Court of Auditors needs a classified document that it has received, or is authorised to access, to be downgraded or declassified the Court shall consult the originator to ask if the originator can provide a downgraded or declassified version of the document.

[3] Pursuant to Decision No 12-2005 of the Court of Auditors regarding public access to Court documents, as amended by Decision No 14-2009 (OJ 2009/C 67/1).

Article 4. **Personnel security**

1. By virtue of their functions, the Members of the Court of Auditors shall be authorised to have access to all EUCI, and to take part in meetings at which EUCI is handled. The Members shall be informed of their security obligations regarding the protection of EUCI and shall acknowledge their responsibility in writing for protecting such information.

2. A member of Court of Auditors staff, whether official, staff subject to the Conditions of Employment of Other Servants, or SNE, shall only be granted access to EUCI after:

   i. their need to know has been established;

   ii. they have been informed of the security rules for protecting EUCI and the relevant security standards and guidelines, and have acknowledged their responsibility in writing for protecting such information; and

   iii. in the case of information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above, they have been security cleared and granted authorisation for access.

3. The procedure for determining whether an official or other member of Court of Auditors staff can be authorised to access information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above, account being taken of the individual's loyalty, integrity and reliability, and after obtaining assurance from the competent authorities of a Member State as referred to in Article 2(n), shall be laid down in a delegated decision taken in accordance with Article 10(10). Decisions to grant authorisation for access shall be taken by the Director of Human Resources, Finance and General Services of the Court of Auditors.

4. The Director of Human Resources, Finance and General Services of the Court of Auditors may issue PSCCs specifying the classification level for which individuals may be granted access to EUCI (CONFIDENTIEL UE / EU CONFIDENTIAL or above), the period of validity of the corresponding authorisation for access and the expiry date of the PSCC.

5. Only persons with the authorisation referred to in paragraph 2(iii) above and Members of the Court of Auditors pursuant to paragraph 1 above may take part in meetings at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is handled. The Court of Auditors and the originator shall make the practical arrangements for such meetings on a case-by-case basis.

6. The departments of the Court of Auditors that are responsible for organising meetings at which information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above is to be handled shall inform the information security authority in good time of the meeting dates, times and locations, with lists of participants.

7. Any individual who is in possession of EUCI without due authorisation and/or with no proven need to know must report the situation to the information security authority as soon as possible and ensure that the EUCI is protected as required by this Decision.

Article 5. **Physical security measures to protect classified information**

1. 'Physical security' means the use of physical and technical protective measures to prevent unauthorised access to EUCI.

2. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions, and to allow for segregation of staff in their access to EUCI on a need-to-know basis. These measures shall be determined on the basis of a risk management procedure, in accordance with this Decision.

3. Areas where EUCI is handled or stored shall be subject to regular inspection by the competent Court of Auditors' security authority.

4. Only equipment or devices that comply with the rules applicable within the EU institutions, agencies or bodies for protecting EUCI shall be used to handle and store EUCI.

5. Court of Auditors staff may access EUCI classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above, or the equivalent in Secured Areas outside Court of Auditors' premises.

6. 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. Unless specifically agreed by the originator, this EUCI shall not be handled or stored on the Court of Auditors' premises and shall not be duplicated or translated by the Court of Auditors.

7. RESTREINT UE/EU RESTRICTED information received shall be recorded by the Court of Auditors. Consultation of information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above, or the equivalent, off Court of Auditor premises shall be registered for security purposes.

8. EUCI classified as RESTREINT UE/EU RESTRICTED may be stored in suitable locked office furniture in an Administrative Area or a Secured Area. EUCI classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be stored under a service level agreement in a security container in a Secured Area of another EU institution in Luxembourg.

9. When outside the registry, EUCI shall be transferred between departments and premises as follows:

   a) as a general rule, EUCI shall be transmitted by electronic means protected by cryptographic products approved in accordance with Article 6(8);

   b) if not transmitted as described in point (a), EUCI shall be transferred using a data carrier (e.g. USB memory stick, CD, hard disk) protected by cryptographic products approved in accordance with Article 6(8), or as a paper copy in an opaque sealed envelope.

10. RESTREINT UE/EU RESTRICED information may be destroyed by the holder, subject to the archiving rules applicable in the Court of Auditors. Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be destroyed only by the Registry Control Officer when so instructed by the holder or by a competent authority in accordance with the archiving rules applicable at the Court of Auditors. Documents classified as SECRET UE/EU SECRET shall be destroyed in the presence of a witness with security clearance corresponding at least to the classification level of the document to be destroyed. The Registry Control Officer and the witness, where one is required to be present, shall sign a record of destruction, which shall be filed in the registry. The Registry Control Officer shall keep records of the destruction of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET documents for at least five years.

11. The physical security authority and the information security authority shall draw up a joint plan, taking local conditions into account, for the safeguarding of EUCI in times of crisis, including, where necessary, plans for its destruction or evacuation in the event of an emergency. They shall issue such instructions as they deem appropriate to prevent EUCI from falling into the hands of unauthorised persons.

12. Where EUCI needs to be transported physically, the Court of Auditors shall comply with the measures imposed by the originator to protect it against unauthorised disclosure during transport.

13. The physical security measures that shall apply in Administrative Areas where RESTREINT UE/EU RESTRICTED information is handled and stored are set out in the Annex.

Article 6. **Protecting EUCI in communication and information systems**

1. For the purposes of this Article, 'communication and information system' means any system enabling the handling of EUCI in electronic form. A communication and information system shall comprise all the assets required for it to operate, including infrastructure, organisation, personnel and information resources.

2. 'Legitimate user' means a Court of Auditors Member, official, other member of staff or SNE with an established and recognised need for access to a specific information system.

3. The Court of Auditors shall provide assurance that its systems will protect the information they handle to an appropriate degree and will function as they need to, when they need to, under the control of legitimate users. To this end, they shall guarantee appropriate levels of:
   - authenticity: the guarantee that information is genuine and from bona fide sources;
   - availability: the property of being accessible and usable upon request by an authorised entity;
   - confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes;
   - integrity: the property of safeguarding the accuracy and completeness of assets and information;
   - non-repudiation: the ability to prove an action or event has taken place, so that the action or event cannot subsequently be denied.

   This assurance shall be based on a risk management process. 'Risk' means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact. The risk management process shall consist of the following steps: threat and vulnerability identification, risk assessment, risk treatment, risk acceptance and risk communication.

   - 'Risk assessment' consists of identifying threats and vulnerabilities and carrying out the corresponding risk analysis, i.e. assessing probability and impact.
   - 'Risk treatment' consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring risk.
   - 'Risk acceptance' is the decision to agree to the further existence of a residual risk after risk treatment.
   - 'Residual risk' means the risk which remains after security measures have been implemented, given that not all threats can be countered and not all vulnerabilities can be eliminated;
   - 'Risk communication' consists of raising awareness of risks among the user community of a communication and information system, informing approval authorities of those risks and reporting them to operating authorities.

4. All electronic devices and equipment used for handling EUCI shall comply with the rules applicable for protecting EUCI. Preference shall be given to electronic devices and equipment that have already been accredited by another EU institution, agency or body. Devices shall be guaranteed secure throughout their full life-cycle.

5. The Court of Auditors' communication and information system for handling EUCI shall be accredited by an appropriate authority. To this end, the Court of Auditors shall seek a Service Level Agreement (SLA) with a security accreditation authority of an EU institution that has the capability to accredit CIS handling EUCI, with a view to receiving an accreditation statement for RESTREINT UE/EU RESTRICTED information that may be handled in the Court of Auditors CIS, and the corresponding terms and conditions for operation. The SLA shall also refer to the

standards to be applied for the accreditation process and shall be concluded in accordance with the procedure laid down in Article 10(3).

6. In case the Court of Auditors needs to establish its own accreditation process for its CIS, a delegated decision as referred to in article 10(10) of this decision shall establish the process in line with the standards on the accreditation process for CIS handling EUCI in other EU Institutions, agencies and bodies.

7. The responsibility for the preparation of the accreditation files and documentation in line with the applicable standards shall rest entirely upon the CIS System Owner.

8. Where EUCI is protected by cryptographic products, the Court of Auditors shall give preference to products approved by the Council or by the Secretary-General of the Council in its function as crypto approval authority or, otherwise, to those approved by other EU institutions, agencies and bodies for the protection of EUCI.

9. RESTREINT UE/EU RESTRICTED information shall only be handled on electronic devices (such as workstations, printers, photocopiers) which are located in an Administrative Area or a Secured Area. Electronic devices that handle RESTREINT UE/EU RESTRICTED information shall be segregated from other computer networks and protected through appropriate physical or technical measures.

10. All Court of Auditors' staff involved in the design, development, testing, operation, management or usage of CIS handling EUCI shall notify to the Information Security Officer all potential security weaknesses, incidents, breaches of security or compromise which may have an impact on the protection of the CIS and/or the EUCI therein.

Article 7. **Procedure for exchanging and enabling access to classified information**

1. When they are legally required to do so by virtue of the Treaties or legal acts adopted on the basis of the Treaties, the EU institutions, agencies, bodies and offices and national authorities provide on their own initiative or at the written request of the President, the reporting Member(s) or the Secretary-General access to EUCI to the Court of Auditors following the below procedure.

2. Access requests shall be sent to the institutions concerned through the Records office of the Court of Auditors.

3. Where necessary, the Court of Auditors shall conclude an administrative arrangement covering the practicalities for exchanging EUCI or equivalent information.

4. For the purpose of concluding such administrative arrangements, the Court of Auditors shall provide the originator with all necessary information about its information security system. If necessary, an assessment visit can be organised.

5. These administrative arrangements shall be concluded in full compliance with the principles of conferral and sincere cooperation set out in Article 13 of the Treaty on European Union. They shall be concluded in accordance with the procedure laid down in Article 10(4).

6. Where no administrative arrangement exists with a given EU institution, body or agency, a third State or International Organisation on providing classified information to the Court of Auditors, the Court of Auditors shall sign a statement of undertaking to protect the classified information it receives.

Article 8. **Breach of security, loss or compromise of classified information**

1. A breach of security means an act or omission by an individual that is contrary to the security rules laid down in this Decision and its implementing rules.

2. Compromise occurs where, as a result of a breach of security, EUCI has been disclosed in whole or in part to unauthorised persons.

3. Any breach or suspected breach of security shall be reported immediately to the information security authority of the Court of Auditors.

4. Where it is known, or where there are reasonable grounds to assume, that EUCI has been compromised or lost, the information security authority shall inform the Director of Human Resources, Finance and General Services and the Secretary-General of the Court of Auditors. The Director of Human Resources, Finance and General Services shall immediately inform the respective Security Authority of the originator. The above-mentioned Director of the Court of Auditors shall conduct an enquiry, informing the Secretary General of the Court of Auditors and the Security Authority of the originator of the results and of the measures taken to prevent the situation from recurring. Where a Member of the Court of Auditors is concerned, the President of the Court of Auditors shall be responsible for taking action in cooperation with the Secretary-General of the Court of Auditors.

5. Any official or other member of staff of the Court of Auditors who is responsible for a breach of the security rules laid down in this Decision and its implementing rules shall be liable to the penalties provided for in the Staff Regulations and the Conditions of Employment of Other Servants of the European Union.

6. Any Member of the Court of Auditors who fails to comply with the terms of this Decision shall be liable to the measures and penalties provided for in Article 286(6) of the Treaty.

7. Any individual who is responsible for losing or compromising EUCI may be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

Article 9. **Security in the event of external intervention**

1. The Court of Auditors may entrust the performance of tasks that involve or require access to EUCI, by virtue of their contract, to contractors registered in a Member State. This may occur in particular in connection with the maintenance of communication and information systems and the computer network.

2. In the event of external intervention, the Court of Auditors shall take all necessary security measures referred to in paragraph 3 of this article including requesting a facility security clearance to ensure that EUCI is protected by candidates and tenderers throughout the duration of a tendering and procurement procedure, and by contractors and subcontractors throughout the term of a contract. The contracting authority shall ensure that the minimum security standards provided for in this Decision are mentioned in contracts to oblige contractors to comply with them.

3. Security rules, procurement procedures, and templates and models for contracts and subcontracts involving access to EUCI, contract notices, guidance on the circumstances in which facility and staff security clearance is required, programme or project security instructions, security aspects letters, visits, and the transmission and transport of EUCI under such contracts and subcontracts, shall conform to the rules, templates and models established by the European Commission for classified contracts in Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.

Article 10. **Implementation of the Decision and linked Responsibilities**

1. The departments of the Court of Auditors shall take all necessary measures, within the scope of their responsibility, to ensure that, when handling or storing EUCI or any other classified information, they apply this Decision and the relevant implementing rules.

2. The Secretary-General shall be the appointing authority and the authority empowered to conclude contracts of employment for all officials and other staff. The Secretary-General may delegate responsibility to the Director of Human Resources, Finance and General Services for granting officials and other staff authorisation to access information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above, for exercising its function as Security Accreditation Authority and for supervising the Secretariat of the Court as regards handling of EUCI.

3. The Secretary General shall be competent to conclude SLAs on the accreditation of the Court of Auditors' communication and information equipment and systems, on the use of a Secured Area in another EU institution and the procedure for personal security clearances requests for access to EUCI.

4. The Director of Human Resources, Finance and General Services shall be competent to conclude administrative arrangements with the EU institutions, agencies and other bodies for the exchange of EUCI, which the Court of Auditors requires to carry out its mandate. This Director may also conclude administrative arrangements with third States or international organisations on protecting any classified information received.

5. The Director for Human Resources, Finance and General Services shall be competent to sign any statement of undertaking for protecting the EUCI to be provided in the context of an exceptional ad hoc release.

6. The Information Security Officer of the Court of Auditors shall act as information security authority. The Information Security Officer and the persons to whom they delegate all or part of their tasks shall have appropriate security clearance. The information security authority shall assume its responsibilities in close cooperation with the Directorate of Human Resources, Finance and General Services, the Directorate for Information, Workplace and Innovation and the Directorate of the Audit Quality Control Committee (see in particular Articles 4, 6 and 8). The information security authority shall also be responsible for training and awareness-raising meetings on information security, and for periodic inspections to verify compliance with this Decision, including in the event of external intervention and any measures to be taken to ensure compliance.

7. The Head of Security shall be responsible for physical security measures (in particular Article 5).

8. A Records Office set up in the Secretariat of the Court shall be the entry and exit point for information classified as RESTREINT UE/EU RESTRICTED which the Court of Auditors may exchange with other EU institutions, agencies and bodies, Member States. It shall also be the entry and exit point for third States' and international organisations' equivalent information. The Records Office shall be organised as laid down in a delegated decision. The Records Officer shall assume the following main responsibilities:

   a) recording entry and exit of information classified as RESTREINT UE/EU RESTRICTED;

   b) management of dedicated Administrative Areas for recording handling, storing and consulting EUCI classified RESTREINT UE/EU RESTRICTED.

9. A Registry shall be set up under an SLA on the use of the Secured Area of another EU institution. This Registry organised by the Secretariat of the Court under the responsibility of the Court of Auditors' Director for Human Resources, Finance and General Services shall be the entry and exit point for information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above which the Court of Auditors may exchange with other EU institutions, agencies and bodies and Member States. It shall also be the entry and exit point for third States' and international organisations' equivalent information. It shall be equipped with appropriate safes and other security equipment suitable for protecting information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above. The Registry shall be organised as laid down in a delegated decision.

The Registry Control Officer shall have appropriate security clearance and assume the following main responsibilities:

a) management of operations relating to the registration, consultation, preservation, reproduction, translation, transmission, dispatch and, where appropriate, destruction of EUCI;

b) assume any other tasks related to the protection of EUCI defined in a delegated decision.

10. The Administrative Committee shall adopt a delegated decision laying down implementing rules for this Decision. The Information Security Officer shall establish information security guidelines. The Audit Quality Control Committee shall draw up audit guidelines.

Article 11. **Entry into force**

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, 3 June 2021.

For the Court of Auditors

Klaus-Heiner Lehne
President

Annex: PHYSICAL SECURITY MEASURES REGARDING ADMINISTRATIVE AREAS FOR EUCI

ANNEX

PHYSICAL SECURITY MEASURES REGARDING ADMINISTRATIVE AREAS FOR EUCI

1. This Annex contains rules for implementing Article 5 of the Decision. These are minimum rules for the physical protection of Administrative Areas for RESTREINT UE/EU RESTRICTED information at the Court of Auditors: areas which are designated for the recording, storage and consultation of information classified as RESTREINT UE/EU RESTRICTED.

2. The purpose of physical security measures in Administrative Areas is to prevent unauthorised access to those areas as follows:

   a) a visibly defined perimeter shall be established which allows individuals to be checked;

   b) unescorted access shall be granted only to individuals duly authorised by the Court of Auditors' information security authority or another competent authority; and

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

3. The Court of Auditors' information security authority may exceptionally grant access to unauthorised persons, including for work in an Administrative Area, provided this does not entail access to EUCI – which shall remain locked away. Such persons may only enter if accompanied and constantly supervised by the information security authority or the Records Control Officer.

4. The information security authority shall lay down procedures for managing the keys and/or combination settings for all Administrative Areas and secure furniture. The purpose of these procedures shall be to guard against unauthorised access.

5. Combination settings shall be committed to memory by the smallest possible number of individuals who need to know them. Combination settings for secure furniture used for storing RESTREINT UE/EU RESTRICTED information shall be changed:

   - on receipt of a new item of secure furniture;
   - whenever there is a change in personnel knowing the combination;
   - if the setting has been, or is suspected to have been, compromised;
   - if a lock has undergone maintenance or repair;
   - at least every 12 months.

6. The information security authority and the Head of Security shall be responsible for compliance with these rules.