COMMISSION DECISION (EU) 2022/640

of 7 April 2022

on implementing rules for the roles and responsibilities of the principal security actors

THE EUROPEAN COMMISSION,

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

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

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

Whereas:

(1) Decisions (EU, Euratom) 2015/443 and (EU, Euratom) 2015/444 apply to all Commission departments and premises of the Commission.

(2) Where necessary, implementing rules to supplement or support Decision (EU, Euratom) 2015/444 are to be adopted in accordance with Article 60 thereof.

(3) Security measures for protecting EU classified information throughout its life-cycle should be commensurate in particular with its security classification.

(4) Security measures for protecting communication and information systems in the Commission are laid down in Commission Decision (EU, Euratom) 2017/46 ([3]), in particular Article 3 on Principles for IT security in the Commission and Article 9 on System owners.

(5) The objective of implementing rules on the roles and responsibilities of the principal security actors is to provide guidance on the prerequisites and duties that are laid down for those roles in Decisions (EU, Euratom) 2015/443 and (EU, Euratom) 2015/444.

(6) Article 36(7) of Decision (EU, Euratom) 2015/444 lays down a number of additional security-related functions to be assumed by the Commission Security Authority. The tasks related to these functions are laid down in this Decision.

(7) Local Security Officers and Registry Control Officers have specific responsibilities for the protection of EU classified information in their departments according to Decision (EU, Euratom) 2015/444.

(8) On 4 May 2016, the Commission adopted a decision ([4]) empowering the Member of the Commission responsible for security matters to adopt, on behalf of the Commission and under its responsibility, the implementing rules provided for in Article 60 of Decision (EU, Euratom) 2015/444; subsequently on 13 April 2021, the Member of the Commission responsible for security matters adopted, on behalf of the Commission and under its responsibility, a decision ([5]) subdelegating these implementing rules to the Director-General of the Directorate-General for Human Resources and Security,

([1]) OJ L 72, 17.3.2015, p. 41.
([2]) OJ L 72, 17.3.2015, p. 53.
([3]) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).
([4]) Decision C(2016) 2797 final of 4 May 2016 on an empowerment relating to security.
([5]) Decision C(2021) 2684 final of 13 April 2021 granting a subdelegation of powers granted in Commission Decision C(2016)2797 on an empowerment relating to security.

HAS ADOPTED THIS DECISION:

CHAPTER 1

General Provisions

Article 1

Subject matter and scope

1. This Decision sets out the roles and responsibilities of the principal security actors who are responsible for protecting EU classified information (EUCI) in the Commission under Decisions (EU, Euratom) 2015/443 and (EU, Euratom) 2015/444.

2. This Decision shall apply to all Commission departments and in all premises of the Commission.

CHAPTER 2

The Directorate-General for Human Resources and Security

Article 2

Commission Security Authority

1. The Director of the Security Directorate in the Directorate-General for Human Resources and Security shall be the Commission Security Authority (CSA) referred to in Article 7 of Decision (EU, Euratom) 2015/444.

2. The CSA shall perform its functions in the following areas as laid down in Decision (EU, Euratom) 2015/444, in accordance with Articles 3 to 7 of this Decision:

(a) personnel security;

(b) physical security;

(c) management of EUCI;

(d) accreditation of any communication and information system (CIS) handling EUCI;

(e) industrial security; and

(f) exchange of classified information.

3. The CSA shall provide mandatory training for the Local Security Officers (LSOs), deputy LSOs, Registry Control Officers (RCOs) and deputy RCOs on their responsibilities and duties.

Article 3

Information Assurance Authority

The Information Assurance Authority shall be responsible for the following activities in relation to the protection of EUCI:

(a) developing information assurance security policies and security guidelines and monitoring their effectiveness and pertinence;

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

(c) ensuring that information assurance measures comply with the Commission's security and procurement policies as appropriate;

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

(e) consulting with system owners, system providers, security actors and representatives of users with respect to information assurance security policies and security guidelines.

Article 4

Security Accreditation Authority

1. The CSA shall be responsible for accrediting Secured Areas that meet the requirements of Article 18 of Decision 2015/444 and CISs for handling EUCI.

2. Commission departments shall consult the Security Accreditation Authority in coordination with their LSO and their LISO as appropriate whenever a department intends to:

(a) construct a Secured Area;

(b) implement a CIS to handle EUCI;

(c) install any other equipment for the handling of classified information, including connections to a third party CIS.

The SAA shall provide advice in respect of these activities during both the planning and the construction or development processes.

3. EUCI shall not be handled in a Secured Area or CIS before the Security Accreditation Authority has issued an accreditation at the appropriate level of EUCI.

4. The requirements for accrediting a Secured Area shall include:

(a) approval of the plans for the Secured Area;

(b) approval of any contracts for works performed by external contractors, taking into consideration the provisions on industrial security such as any requirements for security clearances of the contractors and their staff;

(c) availability of all requisite declarations and certificates of conformity;

(d) a physical inspection of the Secured Area to verify that the building materials and methods, access controls, security equipment and any other items comply with the requirements issued by the CSA;

(e) validation of the countermeasures against electromagnetic radiation for any technically Secured Area;

(f) approval of the security operating procedures (SecOPs) for the Secured Area.

5. The requirements for accrediting a CIS handling EUCI shall include:

(a) creation of a System Accreditation Strategy;

(b) validation of the CIS's security plan, based on a risk management approach;

(c) validation of the SecOPs for the CIS;

(d) validation of all other required security documentation, as determined by the Security Accreditation Authority;

(e) approval of any use of encrypting technologies;

(f) validation of the countermeasures against electromagnetic radiation for a CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above;

(g) an inspection of the CIS to verify that the documented security measures are correctly implemented.

6. Following successful fulfilment of the requirements for accreditation, the Security Accreditation Authority shall issue a formal authorisation for the handling of EUCI in the Secured Area or CIS, for a stated maximum level of EUCI and for up to 5 years, depending on the levels of EUCI handled and the risks involved.

7. Upon notification of a security breach or a significant change in the design or security measures of a Secured Area or CIS, the Security Accreditation Authority shall review and, if necessary, may revoke the authorisation to handle EUCI until any identified issues are resolved.

Article 5

TEMPEST Authority

1. TEMPEST security measures shall be implemented to protect CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, and may be implemented for information classified RESTREINT UE/EU RESTRICTED.

2. The TEMPEST Authority shall be responsible for approving the measures taken to protect against compromise of EUCI through unintentional electronic emanations.

3. Upon request from a system owner of a CIS handling EUCI, the TEMPEST Authority shall issue specifications for TEMPEST security measures as appropriate for the classification level of the information.

4. The TEMPEST Authority shall perform technical testing during the accreditation of Secured Areas and CIS for handling EUCI at the level of CONFIDENTIAL UE/EU CONFIDENTIAL or above and, upon successful testing, issue a TEMPEST certificate.

5. A TEMPEST certificate shall specify at least:

(a) the date of the test;

(b) a description of the TEMPEST security measures, with plans of the premises;

(c) the expiry date of the certificate;

(d) any changes that will invalidate the certification;

(e) the signature of the TEMPEST Authority.

6. An LSO or a meeting organiser with the responsibility for organising a classified meeting, in coordination with the LSO, may request the TEMPEST Authority to test meeting rooms in order to ensure that they are technically secured.

Article 6

Crypto Approval Authority

1. The Crypto Approval Authority shall be responsible for approving the use of encrypting technologies.

2. The Crypto Approval Authority shall issue guidance on the requirements for the use and approval of encrypting technologies.

3. The Crypto Approval Authority shall approve the use of encryption solutions on the basis of a request from the system owner. The approval shall be based upon a satisfactory evaluation of at least:

(a) the security needs of the information to be protected;

(b) an overview of the CIS involved in the solution;

(c) an assessment of the inherent and residual risks;

(d) a description of the proposed solution;

(e) the SecOPs for the encryption solution.

4. The Crypto Approval Authority shall keep a register of approved encryption solutions.

Article 7

Crypto Distribution Authority

1. The Crypto Distribution Authority shall be responsible for distributing cryptographic materials used for protecting EUCI (mainly encryption equipment, cryptographic keys, certificates and related authenticators) to the following:

(a) users or departments inside the Commission for CIS that are administered by external parties;

(b) users or organisations outside the Commission for CIS that are administered by the Commission.

2. The Crypto Distribution Authority may delegate the distribution of cryptographic materials for third parties to other departments in line with Article 17(3) of Decision 2015/443.

3. The Crypto Distribution Authority shall ensure that all cryptographic materials are sent via secure channels that protect against and show evidence of any tampering, in line with the security rules applicable for the level of classification of the EUCI that will be protected by those materials.

4. The Crypto Distribution Authority shall provide guidance to the LSO and, where relevant, the Local Informatics Security Officer of each Commission department that is involved in the production, distribution or use of the cryptographic materials.

5. The Crypto Distribution Authority shall ensure that suitable SecOPs are established for the distribution process.

CHAPTER 3

Commission departments

Article 8

Heads of Department

1. Each Head of Department shall appoint:

(a) an LSO and one or more deputies where appropriate for the department or cabinet;

(b) an RCO and one or more deputies where appropriate for each department that operates an EUCI registry;

(c) a system owner for each CIS handling EUCI.

2. The Head of Department shall request approval from the Director of the Security Directorate of the Directorate-General for Human Resources and Security prior to the appointment of LSOs, deputy LSOs, RCOs and deputy RCOs.

3. The Head of Department shall identify all posts requiring clearance to access EUCI, in consultation with the LSO. Candidates for such posts shall be informed of the requirement for clearance during the recruitment process.

4. The head of any department holding EUCI shall be responsible for activating emergency destruction and evacuation plans when necessary. The plans shall include an alternative for situations when the Head of Department cannot be contacted.

Article 9

System owners of CIS handling EUCI

1. The system owner shall contact the Security Accreditation Authority as early as possible in a project to implement a CIS handling EUCI in order to determine the relevant security standards and requirements, and to begin the process of security accreditation.

2. The system owner shall ensure that the security measures satisfy the requirements of the Security Accreditation Authority and that the CIS does not handle EUCI before it has been accredited.

3. The system owner shall contact the Crypto Approval Authority for approval to use any encrypting technologies. System owners shall not operate encrypting technologies in production systems without prior approval.

4. The system owner shall consult the department's LISO for matters relating to the security of CISs.

5. The system owner shall review the security measures that are applied to a system, including its security plan, at least annually.

6. Where a security incident occurs in a CIS whereby it is indicated that the CIS can no longer adequately protect EUCI, the system owner shall inform the LSO and immediately contact the Security Accreditation Authority for advice on how to proceed. In this case, accreditation may be suspended and the system may be taken out of operation until suitable corrective action has been taken.

7. The system owner shall give the Security Accreditation Authority full support at all times in the latter's duties relating to the accreditation of the CIS.

Article 10

Information Assurance Operational Authority

The Information Assurance Operational Authority for each CIS shall:

(a) establish security documentation in line with security policies and guidelines, in particular the security plan, the SecOPs related to the system and the cryptographic documentation within the CIS accreditation process;

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

(c) participate in selecting TEMPEST security measures and devices, if required in the security plan, and, in cooperation with the TEMPEST Authority, ensure that they are securely installed and maintained;

(d) monitor implementation and application of the SecOPs related to the operation of the system;

(e) manage and handle cryptographic products, in collaboration with the Crypto Distribution Authority, to ensure the proper custody of cryptographic materials and controlled items and, if required, ensure the generation of cryptographic variables;

(f) conduct security analysis, reviews and tests, in particular to produce the relevant risk reports, as required by the Security Accreditation Authority;

(g) provide CIS-specific Information Assurance training;

(h) implement and operate CIS-specific security measures.

CHAPTER 4

Local Security Officer

Article 11

Appointment of the LSO

1. The LSO and deputy LSOs shall be officials or temporary agents.

2. All LSOs and deputy LSOs shall hold a valid security authorisation to access EUCI up to the level of SECRET UE/EU SECRET, and up to the level of TRES SECRET UE/EU TOP SECRET where necessary. The LSO or deputy LSO shall obtain the security authorisation before their appointment.

3. Commission Representations may request the CSA to grant an exception to the requirements set out in paragraphs 1 and 2.

Article 12

Security operating procedures for Secured Areas

1. The LSO of the Commission department concerned shall draw up SecOPs for each Secured Area under their responsibility.

2. The LSO shall ensure that the SecOPs include the following requirements:

(a) only staff members with a valid security authorisation and an established need to access documents classified as CONFIDENTIEL UE/EU CONFIDENTIAL or higher shall be permitted unescorted access to a Secured Area during office hours;

(b) unescorted access to a Secured Area out of office hours shall only be granted to the LSO of the department, the RCO(s) of the Secured Area, their deputies, and authorised staff from the Security Directorate of the Directorate-General for Human Resources and Security;

(c) recording and communication devices such as mobile phones, computers, cameras or other smart devices shall not be allowed inside Secured Areas without prior authorisation from the CSA; any derogation shall be requested from the CSA in advance; the LSO shall act as the point of contact;

(d) all internal or external personnel who require access to a Secured Area but do not fulfil the criteria set out in point (a) above shall be escorted and supervised at all times by a duly authorised staff member; all such access to a Secured Area shall be recorded in a log book kept at the entrance to the Secured Area;

(e) the LSO shall ensure that the intrusion detection systems monitoring a Secured Area are active and properly functioning at all times, and shall manage all related passwords, keys, PINs or other access and authentication mechanisms.

(f) alarms in a Secured Area shall be reported to the Security Directorate of the Directorate-General for Human Resources and Security, which shall immediately notify the LSO;

(g) the LSO of the department where the Secured Area is located shall keep a record of each intervention following an alarm or a security incident;

(h) procedures shall be in place to cover the event of an alarm or other emergency situation inside the Secured Area, including evacuation of personnel and ensuring a rapid response from an emergency team under the authority of the CSA and external emergency services as necessary;

(i) the LSO shall immediately report any breach of security that occurs inside or involving a Secured Area to the CSA in order to determine the appropriate response;

(j) individual offices, rooms and safes within a Secured Area shall be kept locked whenever they are left unattended;

(k) staff shall avoid discussing classified information in corridors or other common areas of the Secured Area when non-authorised individuals are in the vicinity.

Article 13

Security keys and combinations

1. The LSO shall have overall responsibility for ensuring the proper handling and storage of keys and combinations used in or to access Secured Areas. Keys and combinations shall be stored in a security container and shall be protected to at least the same level as the material to which they give access.

2. The LSO shall maintain a register of security containers and strong rooms, together with an up-to-date list of all staff members who have unescorted access to them.

3. The LSO shall maintain a register of keys for security containers and strong rooms, including the staff members to whom they are allocated. A receipt shall be kept for each key that is issued, including the key identification, recipient, date and time.

4. Keys and combinations shall only be issued to staff who have a need to know and who have been granted the appropriate authorisation to access EUCI. The LSO shall retrieve any key when those conditions are no longer met.

5. The LSO shall keep spare keys and a written record of each combination setting in individual sealed, opaque, signed and dated envelopes to be provided by the staff member responsible for the keys. Those envelopes shall be kept in a security container that is rated for the highest classification of material that is stored in the relevant container or strong room.

6. If, upon a change of combination or key rotation, an envelope shows evidence of tampering or damage, the LSO shall treat that as a security incident and immediately inform the CSA.

7. Changes to the combination settings of security containers in Secured Areas shall be performed under the supervision of the LSO. Combinations shall be reset at least every 12 months and whenever:

(a) a new container is received or a new lock is installed (in particular, default combinations shall be changed immediately);

(b) a compromise is suspected or has occurred;

(c) access is no longer required by a person possessing a combination.

8. The LSO shall keep a record of the dates of the combination changes referred to in paragraph 7.

Article 14

EUCI emergency evacuation and destruction plans

1. The LSO shall assist the Head of Department in establishing emergency evacuation and destruction plans for EUCI, based on guidance provided by HR.DS.

2. The LSO shall ensure that any equipment necessary for the operation of the plans provided for in paragraph 1 is readily available and kept in good working order.

3. The LSO, together with the officials nominated in the plans provided for in paragraph 1, shall review the state of preparedness of the plans at least every 12 months and shall take any action necessary to update them.

Article 15

Security authorisations

1. The LSO shall maintain a record of all posts within the department that require a Commission security authorisation and the staff occupying those posts. The requirement for a security authorisation must be specified in the vacancy notice during the recruitment process and notified to the candidate during the interview.

2. The LSO shall oversee all requests for security authorisations for access to EUCI. The LSO shall be the contact point within the department and shall liaise with the CSA for the security authorisations.

3. The LSO shall initiate the request to launch the security authorisation procedure in respect of the staff member concerned and shall ensure that the staff member returns the national security clearance questionnaire promptly to the CSA.

4. The LSO shall ensure that security cleared staff members in the department follow the mandatory EUCI briefing in order to obtain their security authorisation.

5. The LSO shall regularly liaise with the human resources service of the department for information on all changes to posts requiring a security authorisation and shall inform the CSA immediately of any such change.

6. The LSO shall inform the CSA of the arrival of a new staff member holding an existing security clearance to take up a post that requires a security authorised staff member.

7. The LSO shall ensure that staff members in the department complete the procedure to renew a security clearance by the required deadline. Any staff member who refuses to complete the procedure shall be obliged to transfer to a post that does not require a security authorised staff member.

Article 16

EUCI registry

1. Where a department operates an EUCI registry, the LSO shall supervise the activities of the RCOs regarding the handling of EUCI and compliance with the security rules on protecting EUCI.

2. The LSO shall perform the following checks at least every 12 months and upon a change of an RCO or deputy RCO:

(a) a check on a sample of documents in the EUCI registry to confirm their status and the accuracy of the classified documents register;

(b) a check on a sample of receipts and transmission slips for the distribution of EUCI to and from the EUCI registry;

(c) a check on a sample of destruction certificates.

3. On at least a monthly basis, the LSO shall perform spot checks on the classified documents register and on classified documents received recently to ensure that documents are being correctly registered.

4. All checks shall be recorded in the log of the classified documents register.

Article 17

Other security responsibilities

The other security responsibilities of the LSO shall be set out in a security notice covering in particular the physical security of persons, premises and other assets, and information.

CHAPTER 5

Registry Control Officer

Article 18

Appointment of the RCO

1. The RCO and deputy RCOs shall be officials or temporary agents.

2. All RCOs and deputy RCOs shall hold a valid security authorisation to access EUCI up to the level of SECRET UE/EU SECRET, and up to the level of TRES SECRET UE/EU TOP SECRET where necessary. The RCO or deputy RCO shall obtain the security authorisation before their appointment.

3. Commission Representations may request the CSA to grant an exception to the requirements set out in paragraphs 1 and 2.

Article 19

Responsibilities

1. RCOs shall register information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above for security purposes when:

(a) it arrives in or leaves a Commission department; or

(b) it arrives in or leaves a CIS.

2. RCOs shall register all events in the lifecycle of all information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above. RCOs shall also ensure that a record is kept of all information classified as RESTREINT UE/EU RESTRICTED or its equivalent that is exchanged with third countries and international organisations. This shall be done in coordination with the EUCI registry managed by the Secretariat-General.

3. The RCO shall register documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or above in the classified document register and ensure that they are stored securely inside the EUCI registry.

4. The RCO shall assist Commission staff in creating and sending information classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher.

5. When documents classified as CONFIDENTIEL UE/EU CONFIDENTIAL or higher are received from other departments or external parties, the RCO shall ensure that the delivery receipt is duly returned to the originator.

6. Before allowing a member of staff to access a classified document held by the EUCI registry, the RCO shall verify with the LSO that the staff member is security-authorised by the CSA.

7. The RCO shall log all personnel entering and exiting the EUCI registry who are not authorised to have unescorted access and accompany them for the duration of their visit.

8. When a member of staff takes a document for consultation outside the EUCI registry, the RCO shall ensure that he or she is aware of the relevant compensatory security measures and that the member of staff returns the document as soon as it is no longer needed. The RCO shall remind staff to return any such document as soon as possible.

9. The EUCI registry shall issue a courier certificate if classified documents are hand-carried outside the country in which the registry is located.

10. Detailed instructions for RCOs on registering classified documents shall be set out in a security notice.

Article 20

Downgrading and declassifying

The RCO shall assist the originating departments in the process of reviewing registered EUCI to ascertain whether the original classification level is still appropriate, or whether the document can be downgraded or declassified.

Article 21

Destruction

1. RCOs shall be responsible for destroying information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above by approved means, where appropriate in the presence of security-cleared witnesses.

2. RCOs shall record any destruction of information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above in the classified document register and keep the corresponding destruction certificates in the EUCI registry.

Article 22

Additional tasks

1. The RCO shall provide all necessary assistance to the LSO when the LSO performs supervisory activities in the EUCI registry.

2. The RCO shall report any suspected or actual security incidents to the LSO, who shall in turn report them to the CSA.

3. The RCO of the EUCI registry of a Commission department organising a classified meeting at the level CONFIDENTIEL UE/EU CONFIDENTIAL or higher shall prepare the EUCI that will be handled during the meeting and shall coordinate with the meeting organiser to ensure that all documents and receipts are handled in line with the relevant rules.

CHAPTER 6

Final Provisions

Article 23

Transparency

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

Article 24

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

Done at Brussels, 7 April 2022.

For the Commission,
On behalf of the President,
Gertrud INGESTAD
Director-General
Directorate-General for Human Resources and Security