Council of the European Union

Brussels, 29 March 2022
(OR. en)

7670/22
ADD 3

Interinstitutional File:
2022/0084 (COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	22 March 2022
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2022) 119 final - Annex 3
Subject:	ANNEX 3 to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information security in the institutions, bodies, offices and agencies of the Union

Delegations will find attached document COM(2022) 119 final - Annex 3.

Encl.: COM(2022) 119 final - Annex 3

EUROPEAN
COMMISSION

Brussels, 22.3.2022
COM(2022) 119 final

ANNEX 3

ANNEX

to the

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on information security in the institutions, bodies, offices and agencies of the Union

{SWD(2022) 65 final} - {SWD(2022) 66 final}

ANNEX III

Measures for the physical protection of European Union classified information ('EUCI')

Equipment and organisational measures for the physical protection of EUCI

1. An Administrative Area must meet the following requirements:

   (a) have a visibly defined perimeter which allows individuals and, where possible, vehicles to be checked;

   (b) ensure that windows that might allow unauthorised visual access to EUCI within the area are made opaque or equipped with blinds, curtains, or other coverings;

   (c) unescorted access is to be granted only to individuals who are duly authorised by the Security Authority of the Union institution or body concerned;

   (d) all other individuals are escorted at all times or be subject to equivalent controls.

2. In addition to the requirements provided in point 1, a Secured Area must meet the following requirements:

   (a) have a visibly defined and protected perimeter through which entry and exit is controlled at all times;

   (b) be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment;

   (c) be equipped with access control and real time monitoring intrusion detection system ('IDS') combined with response security personnel;

   (d) be inspected at the end of normal working hours and at random intervals outside normal working hours where it is not occupied by duty personnel on a 24-hour basis and there is no real time monitoring IDS in place;

   (e) be managed by trained, supervised and appropriately security cleared security personnel;

   (f) have security operating procedures including the following elements:

      (i) the level of EUCI which may be handled, discussed and stored in the area;

      (ii) the surveillance and protective measures to be maintained;

      (iii) the individuals authorised to have unescorted access to the area by virtue of their authorisation to access EUCI and need-to-know;

      (iv) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area;

      (v) any other relevant measures and procedures.

3. Where entry into a Secured Area constitutes direct access to the classified information contained in it, the area must be established as a Class I Area and where that is not the case the area must be established as a Class II area.

   For both classes of Secured Area referred to in the first subparagraph and in addition to the requirements provided in point 2, the Security Department/Officer of the Union institution or body concerned must clearly indicate the level of the highest

security classification of the information normally held in the area and must clearly define a perimeter which allows individuals and, where possible, vehicles to be checked.

Union institutions and bodies must ensure that individuals accessing a Secured Area fulfil the following criteria:

(a) require specific authorisation to enter the area;

(b) be escorted at all times;

(c) be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible.

4. A Secured Area protected against passive and active eavesdropping must be designated as a technically Secured Area. The following requirements apply in addition to those for Secured Areas:

(a) it must be equipped with an IDS, be locked when not occupied and be guarded when occupied. Any keys must be managed in accordance with Article 29(3);

(b) it must be inspected regularly, physically or technically, or both, by the Security Authority of the Union institution or body concerned. Such inspections must also be conducted following any unauthorised entry or suspicion of such entry;

(c) it must have appropriate acoustic and TEMPEST protection.

5. All persons entering technically Secured Areas must comply with the requirements set out in point 3.

6. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.

7. Strong rooms must be constructed within Secured Areas. A strong room is a room with reinforced physical construction where the Security Authority of the Union institution or body concerned approves the walls, floors, ceilings, windows and lockable doors. Such rooms must afford equivalent protection to a security container approved for the storage of EUCI of the same classification level.

Physical protective measures for handling and storing EUCI

8. EUCI which is classified RESTREINT UE/EU RESTRICTED must be handled and stored in any of the following areas:

(a) in a Secured Area;

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals;

(c) outside a Secured Area or Administrative Area provided the holder has undertaken to comply with compensatory measures decided by the Security Authority of each Union institution and body.

9. EUCI which is classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside an Administrative Area or a Secured Area provided the holder has undertaken to store the documents concerned in appropriate locked office furniture when they are not being read or discussed.

10. Union institutions and bodies may handle and store RESTREINT UE/EU RESTRICTED information outside their sites provided the relevant information be protected appropriately. For such purpose, Union institutions and bodies must comply with the measures provided in point 8(c).

11. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information must be handled and stored in one of the following areas:

    (a) in a Secured Area;

    (b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals;

    (c) outside a Secured Area or an Administrative Area where limited in volume and time and provided the holder has undertaken to comply with compensatory measures decided by the Security Authority of the Union institution or body concerned. In addition, the holder of EUCI must take the following steps:

        (i) notify the relevant registry of the fact that classified documents are being handled outside protected areas;

        (ii) keep the document under their control at all times.

12. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information must be stored in a Secured Area accredited to that level by the competent Security Accreditation Authority of the Union institution or body concerned, either inside a security container or inside a strong room.

13. Documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher can only be copied by the relevant Registry.

14. TRES SECRET UE/EU TOP SECRET information must be handled and stored in a Secured Area accredited to that level. To that end, Union institutions and bodies may conclude the necessary arrangements to use a Secured Area hosted and accredited to the appropriate level by the Security Accreditation Authority of another Union institution and body.

15. TRES SECRET UE/EU TOP SECRET information must be stored in a Secured Area, accredited to that level by the Security Accreditation Authority of the competent Union institution or body concerned, under one of the following conditions:

    (a) in a security container approved by the Security Authority of each Union institution and body with one of the following supplementary controls:

        (i) continuous protection or verification by cleared security staff or duty personnel;

        (ii) an approved IDS in combination with security response personnel.

    (b) in an IDS equipped strong room in combination with security response personnel.