



Council of the
European Union

Brussels, 19 October 2023
(OR. en)

13090/23

LIMITE

CSC 447

Interinstitutional File:
2022/0084 (COD)

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	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 <i>- Articles 9-17 and Annex I on non-classified information</i>

1. Following the discussions which took place at the CSC meeting on 5 July 2023, the GSC has prepared a revised draft version of the Chapters 3 and 4 of the Commission's original proposal, covering articles 9-17 and Annex I. The new text can be found in Annex to this note. New text compared to the original is in **bold underlined**, deletions are marked in ~~striketrough~~.
2. The text of the original Commission proposal has been reorganised: Chapter 3 (Information assurance and communication and information systems (CISs)) has been merged with Chapter 4 on non-classified information with a view to having all provisions on non-classified information under a single Chapter. Annex I on protective measures for handling sensitive non-classified information has also been merged into the main body of the text to avoid overlap with the provisions in the articles in the main text.

3. The proposal introduces revised definitions for all three categories of non-classified information – public, normal and sensitive non-classified information. As regards public information, making information available to the public shall be subject to a decision of the Union institutions and bodies. In the case of normal and sensitive non-classified information, the revised definitions present a different approach that focuses on the existing legal obligations of EUIBAs to protect information, depending on its content and – in the case of sensitive non-classified information - on the possible negative impact of its unauthorised disclosure.
4. Furthermore, at a later stage, delegations could consider improving the terminology for the proposed three categories of non-classified information.
5. The proposal introduces several changes to the Commission’s original text in the sense that it obliges to protect all non-classified information, including the availability and integrity of public information. This change is meant to clarify that scenarios such as fake news, distribution of malware to the Member States’ administrations, attached to EU documents or compromise of other pieces of information are covered. For non-public non-classified information, the compromise of integrity and availability is also key, so these aspects should be addressed next to the protection of confidentiality.
6. The proposal, which establishes an obligation to mark normal and sensitive non-classified information, also addresses a problem of ‘legacy’ of unmarked information – unless otherwise decided, information without any marking will be treated as ‘normal’. This change implements a concept of ‘secure default’ and prevents irreversible errors such as publication of normal or sensitive non-classified information that has not been marked.
7. In addition, to simplify the governance of non-classified information issues, and given the provisions on the protection of CIS handling EUCI in another chapter, it is proposed to merge the subgroup on information assurance with the subgroup on non-classified information.
8. Delegations are invited to discuss the proposed revised text at the next meeting of the Council Security Committee on 24 October 2023.

Chapter 3—*[merged with Chapter 4]***Information assurance and communication and information systems (CISs)***Article 9***Principles of information assurance**

- ~~[1.—The assessment of the information security needs shall be taken into account from the start of the creation or at the procurement stage as regards all CISs including in-house, outsourced and hybrid CISs.—moved to new Article 17c(2)]~~
- ~~[2.—Any CIS that handles and stores EUCI shall be accredited in accordance with Chapter 5, Section 5.— to be moved to Chapter 5, Section 5.]Any CIS that handles and stores sensitive non-classified information shall comply with the minimum requirements for sensitive non-classified information in CISs set out in Chapter 4.~~

Article 10—*[merged with Article 16]***Sub-group on information assurance**

- ~~1.—The sub-group on information assurance, as referred to in Article 7(1) point (a), shall have the following roles and responsibilities:~~
- ~~[(a) providing guidance and best practices on the marking, handling and storing of non-classified information in CISs in close cooperation with the Interinstitutional cybersecurity board referred to in Article 9 of Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union;~~
- ~~(b) establishing a metadata scheme for markings and all necessary technical information to contribute to an interoperable and seamless exchange of information across Union institutions and bodies, when interconnecting their respective CISs;~~

~~(c) contributing to the coherence between the information security rules and the cybersecurity baseline across all Union institutions and bodies, referred to in Article 5 of Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. – moved to Article 16(1)]~~

Article 14[- moved to new Article 17 c]

~~Requirements for communication and information systems~~

- ~~1. Union institutions and bodies shall inform users about the confidentiality levels of information that can be handled and stored in a CIS. Where a CIS handles and stores multiple confidentiality levels, metadata and visual markings shall be used to ensure that the different levels can be distinguished.~~
- ~~2. Union institutions and bodies shall identify CIS' users before granting them access to any confidentiality levels other than public use. Users shall be authenticated at a level of assurance that is appropriate to the confidentiality level. Where appropriate, a secure common identification scheme shall be used.~~
- ~~3. Adequate security logs shall be maintained for all CISs to ensure swift investigations in the event of breaches or leaks of information. Such logs shall be maintained for a duration established in the business impact assessment or in the relevant security policies, in a non-repudiable manner.~~

~~Where a CIS handles and stores EUCI, logs related to need to know and access to information shall be maintained until the information is declassified. Security logs shall be searchable and accessible by the Security Authority.~~

- ~~4. Union institutions and bodies shall adopt internal rules on the security of CISs to specify the appropriate security measures in accordance with the security needs of the information to be handled and stored, and taking into account the jurisdictions in which the information is stored, transmitted to and handled. Where applicable, those measures shall include the following:~~
 - ~~(a) restrictions on the geographical location;~~
 - ~~(b) consideration of potential conflicts of interest, boycotts or penalties relating to contractors;~~

- ~~(c) contractual provisions to ensure the security of information;~~
- ~~(d) encryption of information at rest and in transit;~~
- ~~(e) restrictions on the accessibility of Union institutions and bodies' information by contractor personnel;~~
- ~~(f) protection of personal data in accordance with the applicable data protection legislation.~~

~~5. The Union institutions and bodies shall manage their CISs in compliance with the following principles:—~~

- ~~(a) each CIS shall have a system owner or an Information Assurance Operational authority responsible for its security;~~
- ~~(b) an information security *risk management process* covering information security aspects shall be conducted;~~
- ~~(c) the security requirements and security operating procedures shall be formally defined, implemented, checked and reviewed;~~
- ~~(d) information security incidents shall be formally recorded and followed up, in accordance with Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.~~

Chapter 4₃

Non-classified information

Section 1 (new)

General provisions (new)

Article 12a – Basic principles

1. This chapter lays down the basic principles and minimum standards to be applied for the protection and handling of non-classified information.
2. All Union entities shall ensure the authenticity, availability, integrity, non-repudiation and where appropriate, confidentiality of non-classified information by appropriate measures based on assessed security needs.[-see also 12(2), 13(1a), 14(2)]

Article 15

Protection of non-classified information and interoperability

1. Without prejudice to the reporting obligations set out in Regulation EU [XXX] laying down measures for a high common level of cybersecurity in the institutions, bodies, offices and agencies of the Union, Union entities~~institutions and bodies~~ shall establish internal procedures for the reporting and management of any incident or suspected incident that could lead to a compromise of the security of non-classified information.
2. Where required, Union entities~~institutions and bodies~~ shall use the markings provided for in Articles [12, 13 and 14]. Exceptionally, other equivalent markings may be used internally and in relation with their particular counterparts from other Union entities~~institutions and bodies~~ or from the Member States, when all parties agree. Such exception shall be notified to the sub-group on non-classified information, as referred to in Article 7(1), point (b).

3. Contractual safeguards shall be established to ensure the protection of normal and sensitive non-classified information processed by outsourced services **providers**. The safeguards shall be designed to guarantee at least an equivalent level of protection to that provided by this Regulation, and shall include confidentiality and non-disclosure undertakings to be signed by all relevant service providers involved in the provision of the outsourced systems.

Article 16

Sub-group on non-classified information

- 1.** The sub-group on non-classified information referred to in Article 7(1), point (b), shall **provide draft guidance documents to the Interinstitutional Information Security Coordination Group** ~~have, including on~~ the following ~~roles and responsibilities~~ **topics**:
- (a) ~~streamlining~~ the procedures relating to handling and storing ~~of the~~ non-classified information and ~~preparing the~~ **corresponding** relevant guidance, **taking into account the different confidentiality levels**;
 - (b) ~~coordinating with the sub-group on information assurance referred to in Article 7(1), point (a), on matters related to systems handling and storing non-classified information;~~
 - (c) ~~preparing handling instructions for the different confidentiality levels of non-classified information;~~
 - (~~bd~~) ~~assisting Union institutions and bodies in establishing the equivalence between their particular categories~~ **confidentiality levels** of non-classified information and those provided for in Articles [12, 13 and 14];
 - (~~ce~~) ~~facilitating~~ the sharing of non-classified information between Union ~~entities~~ **institutions** and bodies, by providing assistance and guidance;

- (da) ~~[providing guidance and best practices on the marking, handling and storing of **non-classified** information in CISs in close cooperation with the Interinstitutional cybersecurity board referred to in Article 9 of Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union;~~
- (eb) ~~establishing a **the** metadata scheme for markings and all necessary technical information to contribute to an interoperable and seamless exchange of **non-classified** information across Union **entities** institutions and bodies, when interconnecting their respective CISs;~~
- (fe) ~~contributing to the coherence between the information security rules and the cybersecurity baseline **risk management, governance and control framework** across all Union **entities** institutions and bodies, referred to in Article 54 of Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. – moved from Article 10]~~
- (g) **the strength of encryption as referred to in Article 17c(1)(b).**

Section 2 (new)

Categories of non-classified information

Article 12

Public information for public use

1. Information **which Union entities decide to make publicly available** ~~intended for public use or official publication or already disclosed~~ **is public information.** ~~[which can be shared without restrictions inside or outside the Union institutions and bodies, shall be categorised and handled and stored as information for public use. – moved to paragraph 4]~~
2. ~~3.~~ All Union **entities** ~~institutions and bodies~~ shall ensure the **authenticity, availability,** integrity and, **where appropriate, non-repudiation** ~~availability~~ of **public** information ~~for public use~~ by appropriate measures based on its security needs. ~~[-see also Article 12a(2), 13(1a), 14(2)]~~

3. ~~2. **Public information shall be marked visually**~~ Union institutions and bodies may mark with ‘ **[EU] PUBLIC USE**’ ~~the information referred to in paragraph 1.~~
4. **Public information** ~~which can~~ **may** be shared **or exchanged** without restrictions inside or outside the Union ~~entities~~institutions and bodies, shall be categorised and handled and stored as information for public use.

Article 13

Normal information

1. Information intended for use by a Union ~~entity~~institution or body in the execution of its functions **and covered by the obligation of professional secrecy in accordance with Article 339 of the Treaty on the Functioning of the European Union (TFEU)** ~~which is neither sensitive nor classified nor for public use shall be categorised, handled and stored as is~~ normal information. ~~This category covers all normal working level information processed in the Union institution or body concerned.~~
- 1a. **All Union entities shall ensure the authenticity, availability, confidentiality, integrity and non-repudiation of normal information by appropriate measures based on its security needs.** *[– see also Article 12(2), and Article 14(2)]*
2. Normal information may be marked visually or in metadata where necessary to ~~ensure~~ **facilitate** its protection, particularly where ~~shared~~ **exchanged** outside Union ~~entities~~institutions and bodies. The marking ‘EU NORMAL’ or the ‘name or acronym of the Union ~~entity~~institution or body NORMAL’ (adjusted on a case-by-case basis) shall be used in that case.
- ~~[3. Union institutions and bodies shall define standard protective measures for normal information taking into account guidance from the sub-group on non-classified information and any specific risks related to their tasks and activities. – moved and merged to new 17a (1)]~~
3. **Normal information** shall be exchanged outside Union ~~entities~~institutions and bodies only with natural or legal persons having a need-to-know **for the fulfilment of their assigned tasks. They shall be invited to respect handling instructions accompanying the information as referred to in Article 17a(1).**

Sensitive non-classified information

- 1. Information that does not qualify as EUCI but needs to be protected due to legal obligations or because of the negative impact that its unauthorised disclosure may have on legitimate private and public interests, including those of the Union entities, Member States or individuals shall be categorised as sensitive non-classified information.** ~~Union institutions and bodies shall categorise, handle and stored as sensitive non classified all information that is not classified but which they must protect due to legal obligations or because of the harm that may be caused to the legitimate private and public interests, including those of the Union institutions and bodies, Member States or individuals by its unauthorised disclosure.~~
- 2. All Union entities shall ensure the authenticity, availability, confidentiality, integrity and non-repudiation of sensitive non classified information by appropriate measures based on its security needs.** ~~[-see also Article 12a(2) and Article 13(1a)]~~
- 3. Sensitive non-classified information shall be marked visually and in metadata where necessary to facilitate its protection, particularly where exchanged outside Union entities. The marking shall be ['EU SENSITIVE'], except in cases referred to in [Article 15(2)].** ~~2. Each Union institution and body shall identify s by a visible security marking and shall define corresponding handling instructions in accordance with Annex I.~~
- 4. Sensitive non-classified** ~~3. Union institutions and bodies shall protect sensitive non-classified information by applying appropriate measures in respect of its handling and storage. Such information may only be made available inside Union institutions and bodies to individuals with a need-to-know for the fulfilment of their assigned tasks.~~
- 5. Sensitive non-classified information shall be exchanged outside Union entities** ~~institutions and bodies only with natural and legal persons that have a need-to-know. They shall be invited to while respecting the handling instructions accompanying the information as referred to in Article 17a(1). All parties involved shall be made aware of the appropriate handling instructions.~~

Section 3 (new)

Protective measures for handling normal and sensitive non-classified information

[Article 17]

Handling and storing of sensitive non-classified information in CISs

- ~~1. Union institutions and bodies shall ensure that CISs meet the following minimum requirements when handling and storing sensitive non-classified information:~~
- ~~(a) strong authentication shall be implemented to access SNC information and SNC information shall be encrypted in transmission and in storage;~~
 - ~~(b) encryption keys used for storage shall be under the responsibility of the Union institution or body responsible for the operation of the CIS;~~
 - ~~(c) SNC information shall be stored and processed in the Union;~~
 - ~~(d) contractual provisions covering security of staff, assets and information shall be included in any outsourcing contracts;~~
 - ~~(e) interoperable metadata shall be used to record the confidentiality level of electronic documents and to facilitate the automation of security measures;~~
 - ~~(f) measures to prevent and detect data leaks shall be implemented by the Union institutions and bodies to protect sensitive non-classified information;~~
 - ~~(g) security equipment bearing a European cybersecurity certificate shall be used, where available;~~
 - ~~(h) implementation of security measures based on the principles of need-to-know and zero trust to minimise access to sensitive non-classified information by service providers and contractors. — moved to new Article 17c]~~
- ~~2. [Any derogation from the minimum requirements set out in paragraph 1 shall be subject to approval by the appropriate level of management of the Union institution or body concerned, on the basis of a risk assessment covering the legal and technical risks to the security of the sensitive non-classified information. — moved to new Articles 17c(10) and 17d(3)]~~

3. ~~[The Information Assurance Authority of the Union institution or body concerned may check compliance with the principles set out in paragraph 1 at any time during the lifecycle of a CIS. —moved to new Articles 17c(9) and 17d(2).]~~

ANNEX I

Protective measures for handling sensitive non-classified information

Article 17a (new)*[former ANNEX I]*

Minimum requirements for the protection of normal and sensitive non-classified information

Marking and handling of sensitive non-classified information

1. ~~[Documents containing sensitive non-classified information must be marked using security marking and, where relevant, one or more distribution marking or markings specifying the target audience as appropriate. The standard security marking shall be the word ‘SENSITIVE’ in upper case, except in cases referred to in Article 15(2). - integrated with the definitions in Article 13(2) and 14(3)]~~
2. ~~[Documents containing sensitive non-classified information must only be accessible to recipients with a need to know for official purposes. Where distribution markings are used, permission must be requested from the originating Union institution or body to extend the distribution of a document. —moved to new Article 17 b]~~
1. **Union entities shall define specific handling instructions and standard protective measures for normal and sensitive non-classified information, including, where appropriate, distribution markings. In doing so, they shall take into account guidance from the sub-group on non-classified information and any specific risks related to their tasks and activities. Unmarked information is to be considered normal by default, including information created or registered before the date of application of this Regulation which has not been made publicly available.** - moved from Article 13(3) and merged with new text]

2. All persons handling individuals having access to normal and sensitive non-classified information ~~must~~ **shall** be made aware of the handling instructions their obligations to protect the confidentiality of information.
3. Normal and sensitive non-classified information sent by physical post, envelopes or packages shall be addressed to a named individual or the holder of a function, include a return address and not bear any indication on the envelope or package of the non-public content of the information.
4. Documents marked SENSITIVE are downgraded to EU NORMAL or PUBLIC USE, through the removal or striking of the markings.
- 5.4. When Union ~~entities~~institutions and bodies destroy documents containing normal or sensitive non-classified information, this ~~must~~ **shall** be done in such a way that they cannot be easily reconstructed in whole or part. Paper copies ~~must~~ **shall** be shredded and electronic copies must be securely overwritten, physically destroyed or otherwise rendered irrecoverable.

Protection of sensitive non-classified information when working outside the sites of Union institutions and bodies

- ~~[6. Sensitive non-classified information must be protected from eavesdropping and observation during teleworking and missions outside the office, and must not be handled or stored in public. — moved to new Article 17b]~~
- ~~[7. Documents containing sensitive non-classified information must only be handled and stored on equipment or applications that are appropriately secured under the responsibility of Union institutions and bodies. — moved to new Article 17b]~~
- 5.8. Union ~~entities~~institutions and bodies ~~must~~ **shall** provide means to prevent unauthorised persons, including relatives, from accessing or modifying normal and sensitive non-classified information handled or stored by the equipment of a Union ~~entity~~institution or body, when working outside the place of employment.

[9. Union institutions and bodies must instruct their personnel to:

- (a) protect Union institutions or bodies' equipment handling sensitive non-public information from theft, loss and damage and report immediately any such or other adverse security event impacting their devices or the information therein;
- (b) not share their devices with any unauthorised persons;
- (c) not use the equipment for non-work related activities. -moved to new Article 17c(4)]

[10. Union institutions and bodies must ensure that, as far as possible, their equipment or their appropriately secured applications are used to handle and store any sensitive non-classified documents in electronic format outside their sites. Handling of physical copies of sensitive non-classified documents outside the office should be avoided.

11. Where teleconference or videoconference tools are used, Union institutions and bodies must minimise the risk of unauthorised persons seeing or hearing the discussions by appropriately authenticating participants and using encrypted communications tools compatible with the need-to-know.

12. Union institutions and bodies shall provide training to all personnel working remotely on the handling of sensitive non-classified information when working outside the office. - paragraphs 10, 11, 12 to be deleted]

Sharing sensitive non-classified information

13. Documents containing sensitive non-classified information may be shared between Union institutions and bodies without additional formalities.

14. Union institutions and bodies must only share documents containing sensitive non-classified information outside all Union institutions and bodies on the basis of a commitment that binds parties to respect the handling instructions.

~~15.6.~~ Union entities institutions and bodies must shall notify the recipients of normal and sensitive non-classified information of the obligation to not share the information with any parties outside the audience not indicated by in the distribution markings unless allowed by the originator.

- ~~16. Union institutions and bodies must protect the sensitive non-classified information that is provided or shared electronically through appropriate security measures including encryption in transit using appropriate cryptographic mechanisms. [merged into new Article 17d (b)]~~

Article 17b (new)

Minimum requirements for the protection of sensitive non-classified information

- 1. Documents containing sensitive non-classified information shall specify their addressees.**
- ~~2. Documents containing sensitive non-classified information must only be accessible to recipients with a need to know for official purposes. Where distribution markings are used, permission must **shall** be requested from the originating Union **entity** institution or body to extend the distribution of a document. [-moved from Annex I, paragraph 2]~~
- ~~**3.7.** Documents containing sensitive non-classified information ~~must~~ **shall** only be handled and stored on equipment or applications that are appropriately secured under the responsibility of Union **entities** institutions and bodies. [- moved from Annex I, paragraph 7]~~
- ~~**4.6.** Sensitive non-classified information ~~must~~ **shall** be protected from eavesdropping and observation, **in particular** during teleworking and missions outside the office, and ~~must~~ **shall** not be handled or stored in public. [- moved from Annex I, paragraph 6]~~
- 5. Physical copies of sensitive non-classified information and electronic media storing such information shall be stored, whenever possible, on official premises. When not being used, copies shall be stored in locked offices or furniture. When removed from official premises, the information shall be kept under the control of the official at all times, either on their person or in a locked location.**

Minimum protection of normal and sensitive non-classified information in CISs

1. [Union ~~entities~~institutions and bodies shall ensure that CISs meet the following minimum requirements when handling and storing normal or sensitive non-classified information:
 - (a) ~~strong~~ **multifactor** authentication shall be implemented to access ~~SNC~~**sensitive non-classified** information and, **where possible, normal information.** and [SNC information shall be encrypted in transmission and in storage;- moved to Article 17d]
 - ~~[(b) encryption keys used for storage shall be under the responsibility of the Union institution or body responsible for the operation of the CIS;- moved to Article 17d]~~
(b)(e) SNC information shall be stored and processed in the Union; normal and sensitive non-classified information transmitted through the networks not physically controlled by the Union entity shall be protected by cryptographic products recommended by the Interinstitutional Information Security Coordination Group on the basis of a draft guidance document from the sub-group on non-classified information;
 - ~~(c)(d)~~ contractual provisions covering security of staff, assets and information shall be included in any outsourcing contracts;
 - ~~(d)~~**(de) where possible**, interoperable metadata shall be used to record the confidentiality level of electronic documents and to facilitate the automation of security measures;
 - ~~(e)~~ measures to prevent and detect data leaks shall be implemented by the Union ~~entities~~institutions and bodies;
 - ~~(f)~~ security equipment **ICT products** bearing a European cybersecurity certificate **at the level 'substantial' or above** shall be used, where available;
 - ~~(g)~~**(gh)** implementation of security measures based on the principles of need-to-know and zero trust to minimise access to sensitive non-classified information by service providers and contractors.-moved from Article 17(1)]

2. [The assessment of the information security needs shall be taken into account from the start of the creation or at the procurement stage as regards all CISs including in-house, outsourced and hybrid CISs. *—moved from Article 9(1)*]
3. [Union ~~entities~~institutions and bodies shall inform users about the confidentiality levels of information that can be handled and stored in a CIS. Where a CIS handles and stores multiple confidentiality levels, metadata and visual markings shall be used to ensure that the different levels can be distinguished. *—moved from Article 11(1)*]
4. [Union ~~entities~~institutions and bodies ~~must~~ shall instruct their personnel to:
- (a) protect Union ~~entities~~institutions or bodies' equipment handling normal and sensitive non-public information from theft, loss and damage and report immediately any such or other adverse security event impacting their devices or the information therein;
 - (b) not share their devices with any unauthorised persons;
 - (c) not use the equipment for non-work related activities.*—moved from Annex I paragraph 9*]
5. [Union ~~entities~~institutions and bodies shall identify CIS' users before granting them access to any confidentiality levels other than public use. Users shall be authenticated at a level of assurance that is appropriate to the confidentiality level. Where appropriate, a secure common identification scheme shall be used.*—moved from Article 11(2)*]
6. [Adequate security logs shall be maintained for all CISs to ensure swift investigations in the event of breaches or leaks of normal and sensitive non-classified information. Such logs shall be maintained for a duration established in the business impact assessment or in the relevant security policies, in a non-repudiable manner.
- ~~Where a CIS handles and stores EUCL, logs related to need to know and access to information shall be maintained until the information is declassified. Security logs shall be searchable and accessible by the Security Authority. *—moved from Article 11(3)*~~
7. [Union ~~entities~~institutions and bodies shall adopt internal rules on the security of CISs to specify the appropriate security measures in accordance with the security needs of the information to be handled and stored, and taking into account the jurisdictions in which the information is stored, transmitted to and handled. Where applicable, those measures shall include the following:

- (a) restrictions on the geographical location;
- (b) consideration of potential conflicts of interest, boycotts or penalties relating to contractors;
- (c) contractual provisions to ensure the security of information;
- (d) encryption of information at rest and in ~~transit~~ **transmission**;
- (e) restrictions on the accessibility of Union ~~entities~~^{institutions and bodies} information by contractor personnel;
- (f) protection of personal data in accordance with the applicable data protection legislation. –
moved from Article 11(4)]

8. [The Union ~~entities~~^{institutions and bodies} shall manage their CISs in compliance with the following principles:

- (a) each CIS shall have a system owner ~~or~~ **and** an Information Assurance Operational authority responsible for its security;
- (b) ~~an information security risk management process covering information security aspects shall be conducted;~~
- (~~b~~e) the security requirements and security operating procedures shall be formally defined, implemented, checked and reviewed;
- (~~c~~d) information security incidents shall be formally recorded and followed up, in accordance with Regulation EU [XXX] laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. –*moved from Article 11(5)]*

9. [The Information Assurance Authority of the Union ~~entity~~^{institution or body} concerned may check compliance with the principles set out in ~~paragraph 1~~ **this article** at any time during the lifecycle of a CIS. –*moved from Article 17(3)]*

- 10.** [Any derogation from the minimum requirements set out in paragraphs 1 to 10 shall be subject to approval by the appropriate level of management of the Union ~~entity~~ institution or body concerned, on the basis of a risk assessment covering the legal and technical risks to the security of the sensitive non-classified information. — moved from Article 17(2)]

Article 17 d (new)[- text moved from Chapter 4, Article 17]

Minimum protection of sensitive non-classified information in CISs

1. Union ~~entities~~ institutions and bodies shall ensure that CISs meet the following minimum requirements when handling and storing sensitive non-classified information [- moved from Article 17(1)]:
 - (a) **sensitive non-classified SNC information on devices connected to public networks and on storage media without strong physical access control** shall be encrypted. *partially moved from Article 17(1)(a)*
 - (b) encryption keys used for storage shall be under the responsibility of the Union ~~entity~~ institution or body responsible for the operation of the CIS.- moved from Article 17(1)(b) and merged with Annex I, paragraph 16]
- 2.** [3. The Information Assurance Authority of the Union ~~entity~~ institution or body concerned may check compliance with the principles set out in paragraph 1 **this article** at any time during the lifecycle of a CIS.- moved from Article 17(3)]
- 3.** [2. Any derogation from the minimum requirements set out in paragraphs 1 and 2 shall be subject to approval by the appropriate level of management of the Union ~~entity~~ institution or body concerned, on the basis of a risk assessment covering the legal and technical risks to the security of the sensitive non-classified information. — moved from Article 17(2)]