EUROPEAN
COMMISSION

Brussels, 5.3.2019
C(2019) 1903 final

Security Notice

Information assessment and classification

Table of contents

1. INTRODUCTION

This security notice defines the rules for assessing the security needs of information within the Commission, to ensure that information is properly categorised and handled and reduce the risks of information leaks or loss. It implements Article 9(2) of Decision (EU, Euratom) 2015/443[1] ('Decision 2015/443'), which states: '*Security of information, regardless of its form, shall balance transparency, proportionality, accountability and efficiency with the need to protect information from unauthorised access, use, disclosure, modification or destruction.* '

This security notice contributes to the implementation of Article 17 of the Staff Regulations[2], and to compliance with the principle of professional secrecy in Article 339 of the Treaty on the Functioning of the European Union.

The sensitivity of information assets[3] determines their security needs. Security needs are expressed as levels of three key aspects of security: confidentiality, integrity and availability. The scales for all three aspects are given below; this document focuses mostly on the **confidentiality of information**.

The assessment of the security needs helps to determine the appropriate levels of protection in line with the principles of proportionality, accountability and efficiency. The methods for performing this assessment will be covered by additional guidelines.

The transparency of information is addressed through other measures, in particular through Regulation (EC) No 1049/2001[4].

IT security risk assessments, which are based on the defined security needs for Commission communication and information systems (CISs), are covered by Decision 2017/46[5].

Any queries about this security notice should be addressed to the functional mailbox HR MAIL DS3.

2. SECURITY NEEDS

2.1. Confidentiality

The confidentiality of information is assessed according to the damage that unauthorised disclosure may cause to the interests of the Commission, the European Union or one or more of its Member States, or other stakeholders such as businesses

---

1 Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (Official Journal L 72 of 17 March 2015, p. 41).

2 *"An official shall refrain from any unauthorised disclosure of information received in the line of duty, unless that information has already been made public or is accessible to the public."*

3 An information asset is any piece or collection of information that has a value. In this security notice, it indicates a document or a collection of documents that have similar characteristics and security needs.

4 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (Official Journal L 8 of 12 January 2001, p. 1).

5 Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (Official Journal L 6 of 11 January 2017, p. 40).

and European citizens. There are seven levels of information confidentiality which are defined as follows:

Confidentiality level	*Description*
Publicly available (PA)	Information that is, or is ready to be, published[6].
Commission use (CU)	Information that is not for public use and does not fall into higher categories.
Sensitive Non Classified (SNC)	Information that the Commission must protect because of legal obligations or because of its sensitivity. SNC information must be marked[7].
RESTREINT UE/EU RESTRICTED[8]	Information or material designated by an EU security classification at the level RESTREINT UE/EU RESTRICTED, the unauthorised disclosure of which **could be disadvantageous** to the interests of the EU or of one or more of the Member States.
CONFIDENTIEL UE/EU CONFIDENTIAL	Information or material designated by an EU security classification at the level CONFIDENTIEL UE/EU CONFIDENTIAL, the unauthorised disclosure of which **could harm** the essential interests of the EU or of one or more of the Member States.
SECRET UE/EU SECRET	Information or material designated by an EU security classification at the level SECRET UE/EU SECRET, the unauthorised disclosure of which **could seriously harm** the essential interests of the EU or of one or more of the Member States.
TRES SECRET UE/EU TOP SECRET	Information or material designated by an EU security classification at the level TRES SECRET UE/EU TOP SECRET, the unauthorised disclosure of which **could cause exceptionally grave prejudice** to the essential interests of the EU or of one or more of the Member States.

Information relating to the field of atomic energy covered by Articles 24 and 25 of the Treaty establishing the European Atomic Community[9] is called Euratom Classified Information (ECI) and is classified as "Eura – Top Secret", "Eura – Secret", "Eura – Confidential" or "Eura – Restricted" in line with Regulation (Euratom) no 3 of 1958[10].

6 Note that many documents are sensitive before they are published, and so the draft documents may need to be protected at a higher level than the final documents after the date of publication.

7 See the Security Notice on Marking and handling of sensitive non-classified information.

8 The EU security classifications are defined in Article 3 of Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information (Official Journal L 72 of 17 March 2015, p. 53).

9 Official Journal 2C 327 of 26 October 2012, pp. 1-107

10 Official Journal 17 of 6 October 1958, pp. 406-416

The originator[11] of a document[12] or other information asset must determine the appropriate level based on the definitions above (see section 4.1). In case of doubt, particularly when the impact assessment indicates that the information should be classified as EUCI (EU classified information), the Security Directorate of the Directorate-General for Human Resources and Security (HR.DS) should be consulted for advice. It should be noted that selecting a level that corresponds to a lower level of impacts may lead to the information not being protected appropriately, and is therefore forbidden.

Classifying information as EUCI guarantees the continuity of its protection when exchanged with third parties under existing legal arrangements. The EUCI classifications are defined jointly by all EU institutions and in agreement with the Member States.

Information assets can be downgraded[13] or declassified (removal of an EUCI classification) after a date or a specific event such as the publication of a document or the broadcast of a speech[14]. EUCI may also be declassified after a specified time period; if a time period is not specified then the classification level of registered EUCI has to be reviewed at least every 5 years[15].

Section 3 below summarises how to assess the confidentiality level of a document or other information asset and how to handle it.

2.2. Integrity and availability

The levels for integrity and availability are based on a common scale of five ratings or impact levels. The ratings correspond to the worst-case scenarios of the business impact or damage resulting from security breaches. These ratings are especially relevant for the design of IT systems.

Integrity and availability are defined in Article 3 of Decision 2017/46 as follows:

> *'Integrity: the property of safeguarding the accuracy and completeness of assets and information'*

---

[11] Article 1(11) of Decision 2015/444 defines the originator as '"the Union institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the Union's structures'.

[12] Article 1(5) of Decision 2015/444 defines a document as 'any recorded information regardless of its physical form or characteristics'. Taking into account Article 3(a) of Regulation 1049/2001 as interpreted by the jurisprudence, the term is used here to indicate any content whose security needs are being assessed, whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) concerning a matter relating to the policies, activities and decisions falling within the institution's sphere of responsibility, or a record or extract extracted by means of a routine search query from a database. A collection of similar documents, such as an entire database, is considered as an 'information asset'.

[13] Downgrading means either a reduction in the EUCI level (e.g. CONFIDENTIEL UE/EU CONFIDENTIAL to RESTREINT UE/EU RESTRICTED), or a reduction in a non-EUCI confidentiality level (SNC to CU/PA or CU to PA). The removal of an EUCI classification so that a document is no longer classified is termed 'declassification'.

[14] Specific rules on downgrading and declassification in line with Article 26 of Decision 2015/444 will be issued by HR.DS.

[15] Instructions on declassification are given in the relevant implementing rules of Decision 2015/444 (forthcoming).

'Availability: the property of being accessible and usable upon request by an authorised entity'

Integrity includes principles such as authenticity and non-repudiation, and relates to the required level of confidence in the accuracy and the source of information. The availability rating is used to determine the business continuity requirements. The impact definitions in the table below are related to the impacts for confidentiality; hence, for example, levels 4 and 5 are equivalent to the impact ratings for EUCI.

Integrity / Availability Level	***Rating***	***Impact and Scope***
1	Very Low	No or negligible damage to the Commission or other stakeholders.
2	Low	Minor damage to the Commission or other stakeholders[16].
3	Medium	Significant damage to the Commission or other stakeholders.
4	High	Disadvantageous to the interests of the EU or Member States.
5	Very High	Harm, serious harm or exceptionally grave prejudice to the interests of the EU or Member States.

Integrity and availability are typically addressed in the IT security risk management process in line with Article 5 of Decision C(2017) 8841[17].

3. CONFIDENTIALITY LEVELS

This section includes some of the key rules for the handling and marking of sensitive and classified information. The complete rules are given by the relevant security notices or implementing rules as referenced.

3.1. Publicly available (PA)

Description and examples[18]

PA is intended to be, or already has been, released to the public. Examples may include information that is directly available from:

- The Official Journal of the European Union;
- The Register of Commission Documents (RegDoc)[19];

[16] The stakeholders mentioned at levels 2 and 3 do not include Member States. Impacts that are significant at the national level are rated at levels 4 or 5.

[17] Commission Decision C(2017) 8841 of 13.12.2017 laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017 on the security of communication and information systems in the Commission

[18] The examples given in this document are for guidance only, and are not intended to replace a business impact assessment.

[19] The Register of Commission Documents is available at:, https://ec.europa.eu/transparency/regdoc/index.cfm?fuseaction=search.

- Websites providing information for EU citizens;
- Published open calls for tender[20];
- Documents made available under Regulation 1049/2001 on public access to documents.

Information handling and marking

Permission is not required to share or publish PA information, although approval for publication may be required from a press or communications officer before the information is considered to be PA[21]. There are no restrictions on distribution for security reasons.

3.2. Commission use (CU)

Description and examples

CU information is normal, working level information inside the Commission. This information is not particularly sensitive, but it is still covered by Article 17 of the Staff Regulations. Consequently, CU information is not considered to be publicly available.

Unauthorised disclosure of such information may cause a **minor** impact on the Commission, which does not materially affect budgets or cause significant harm. Examples of this type of information may include:

- Internal working documents without a marking;
- Work emails that do not include any sensitive information;
- Contributions to internal information-sharing platforms that do not include any sensitive information;
- Information on the Commission's internal web platform (MyIntraComm) that is available for all staff.

Information handling and marking

Standard office automation tools and CISs may be used to handle CU information. Standard cupboards may be used to store CU information on physical or removable media.

CU information is primarily intended for internal use within the Commission, although it may in some cases be communicated to external entities when required for Commission business, preferably with instructions not to distribute outside their organisation. CU information is not subject to markings.

---

[20] Before their publication, calls for tender may require a higher security level. This is an example of information whose sensitivity changes after a specific event.

[21] Prior to this approval, the information would normally be considered to be CU.

Any information that is more sensitive than CU must be appropriately marked. Consequently, working documents without a marking and emails that are not protected with SECEM (SECure EMail) are to be considered CU by default.

3.3. Sensitive non-classified information (SNC)

Description and examples

SNC is information or material the Commission must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Examples of this type of information may include:

- Commission's Acts (decisions, opinions, recommendations, …) and Commission's proposals (for final adoption of the European Parliament and/or the Council) bearing a marking;
- Some documents related to trade negotiations;
- Some procurement documents, where relevant;
- Sensitive personal information, especially the special categories of data defined in Article 10 of Regulation 2018/1725[22];
- Sensitive business information of third parties;
- Evidence in administrative, competition or criminal investigations;
- Certain audit reports, depending on the subject matter;
- Certain security-related documents, depending on the subject matter;
- Certain sensitive documents forming part of the policy and legislation development process, or parts thereof.

Information handling and marking[23]

SNC information should be secured when not in use, e.g. by storing it in a locked cupboard or in an appropriately secured CIS. Within the Commission, access to SNC information must be restricted to relevant Commission staff, e.g. restricted to the relevant unit or to other staff with a need to know in relation to their specific duties.

Appropriate security markings must be applied to documents to indicate relevant restrictions and handling instructions in line with the security notice on marking and handling of sensitive non-classified information. Emails containing SNC information must be protected using SECEM (within the Commission), or, where possible, using approved protection mechanisms such as S-MIME (with external partners).

---

[22] OJ L 295/39 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

[23] Full instructions are given in the security notice on marking and handling of sensitive non-classified information.

SNC information may be communicated to external entities with formal permission from the author or data owner, with written instructions not to distribute outside a specified audience.

3.4. RESTREINT UE/EU RESTRICTED[24]

Description

RESTREINT UE/EU RESTRICTED is the lowest of the four levels of EUCI and is defined as 'information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of its Member States.'[25]

Information handling and marking

These details are laid down in the implementing rules of Decision 2015/444 on the creation, handling and storage of RESTREINT UE/EU RESTRICTED information[26] ('Decision 2015/444). Access to RESTREINT UE/EU RESTRICTED information may only be granted on a need-to-know basis.

Information classified RESTREINT UE/EU RESTRICTED having originated in the Commission will be considered to be automatically declassified after 30 years[27].

The concept of information assurance (IA) must be applied for CISs handling EUCI, in line with Article 34 of Decision 2015/444. All CISs handling EUCI must be formally accredited and approved for operation by the Commission Security Authority.

RESTREINT UE/EU RESTRICTED data at rest and in transit must be encrypted using approved products[28].

In addition:

- A segregated environment must be used whenever possible;
- A security plan, including the security policy and the security operating procedures, must be defined, implemented, checked and reviewed[29].

---

[24] Eura-Restricted documents are subject to different handling and declassification instructions under Regulation (Euratom) no 3 of 1958.

[25] See Article 3(1) of Decision 2015/444. The individual definitions of the four EUCI levels in this document all come from Article 3(2) of this Decision.

[26] [forthcoming, reference will be provided].

[27] See Article 26(3) of Decision 2015/444 and Regulation (EEC, Euratom) No 354/83 as amended by Council Regulation (EC, Euratom) No 1700/2003.

[28] See the Standard on Cryptography and Public Key Infrastructure, or contact HR.DS for more information.

[29] Note that under Article 9(2) of Decision (EU, Euratom) 2017/46, a security plan is required for all CISs. The requirements are, however, more stringent for CISs handling EUCI.

3.5. CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET

Description

The remaining three EUCI levels are defined in Article 3(2) of Decision 2015/444 as follows:

CONFIDENTIEL UE/EU CONFIDENTIAL means *'information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States'.*

SECRET UE/EU SECRET means *'information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States'.*

TRES SECRET UE/EU TOP SECRET means *'information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States'.*

The security measures are progressively stricter the higher the classification level.

Information handling and marking

Handling and marking rules are given in the following security notices:

- SN04 Creation, handling and storage of CONFIDENTIEL UE/EU CONFIDENTIAL information.
- SN4A Creation, handling and storage of SECRET UE/EU SECRET information.

Access to EUCI at these levels may only be granted on a strict need-to-know basis. Users of this information in the Commission must be security authorised by HR.DS. Documents at these levels must be stored and managed in approved registries.

For TRES SECRET UE/EU TOP SECRET, contact HR.DS.

The rules given under Section 3.4 apply, with increasing stringency depending on the security classification. In addition, proportionate security measures must be implemented to protect against any compromise of information through unintentional electromagnetic emanations (TEMPEST security measures). Contact HR.DS for further information.

4. HORIZONTAL ASPECTS

4.1. Business impact assessments

The data owner or originator must determine the security needs of documents or information assets through a process of assessing the impact of breaches of information security[30]. Where relevant, and especially for information handled in CISs, the levels of integrity and availability must be determined in addition to the level of confidentiality.

[30] When personal data is concerned, the data controller should be involved in this process.

The business impact assessment (BIA) is a necessary first step in the IT security risk management process that is applicable to all CISs in line with Commission Decision C(2017) 8841.

Due to the aggregation of data, multiple documents or CISs containing large quantities of information may need to be protected at a higher level than individual documents.

Security needs relating to availability are also addressed through business continuity. The 'Framework for business continuity management in the Commission'[31] outlines an approach to develop resilience to major disruptions and to ensure that the Commission and its services are able to continue operating.

The methods for assessing the security needs will be covered by additional guidelines from HR.DS.

4.2. Changing confidentiality levels

Changes to the level of confidentiality are performed under the responsibility of the originator, usually by duly appointed management in the originator's department. The rules for making changes should be determined by each department and documented.

When information from various sources is collated, the final product must be reviewed to determine its overall confidentiality level, since it may warrant a higher rating than its component parts.

Often, the level of confidentiality will be reduced after specific milestones, for example after the adoption of a decision by the Commission, when a policy document is finalised and approved, or when an investigation is completed. It is generally difficult to increase the level of confidentiality of information, since once it has been handled and distributed at a lower level, it may not be possible to control all copies.

The document management officer (DMO) of a department may need access to the contents of documents when they are archived. This implies that the DMO may have a need-to-know, but does not permit the DMO to modify the security levels or markings without the authorisation of the originator.

4.3. Personal data protection

Personal data must be protected in accordance with Regulation (EU) 2018/1725, which defines personal data as *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.*

In addition, there are special categories of data, such as *'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and […] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'*, whose processing is generally prohibited.

[31] SEC(2006)899, 12.07.2006.

Personal data that are not public should generally be considered as SNC. In case of doubt, the data protection coordinator (DPC) of the relevant Commission department should be consulted for advice on the level of confidentiality. The security rules described in this document are to be applied without prejudice to the need to handle requests of individuals for access to their personal data or for the exercise of their other rights under Regulation (EU) 2018/1725.

Consequently, duly authorised staff handling requests of individuals for access to their personal data or for the exercise of their other rights under Regulation (EU) 2018/1725 shall have access to the necessary information. The Data Protection Officer (DPO) is authorised to have access to data processing operations on personal data.

4.4. Public access to Commission documents

In line with the principle of transparency (Article 15 TFEU), citizens have the right to the widest possible access to the EU institutions' documents. For the European Parliament, the Council of the EU and the Commission, the rules governing the exercise of this right, including the applicable exceptions, are laid down in Regulation (EC) No 1049/2001.

Information at all levels of security may be disclosed outside the Commission subject to the provisions of Article 9 of Regulation 1049/2001[32] if so required under the provisions of Regulation 1049/2001[33], the Framework Agreement on Relations between the European Parliament and the Commission[34] or the principle of sincere cooperation with the Member States

The security rules described in this document are to be applied without prejudice to the need to carry out a case-by-case assessment in case of a subsequent application for public access to documents under Regulation 1049/2001, taking into account the factual and legal circumstances that are applicable at the time of the decision on access. Consequently, staff handling applications for access to documents under Regulation 1049/2001 need to be able to access Commission documents forming the subject of applications for public access.[35]

Documents bearing an EUCI classification must be declassified when they are disclosed under Regulation 1049/2001, and documents bearing an SNC marking must have the marking removed. Access to documents or parts thereof may be refused based on the exceptions to the right of access defined in Article 4 of Regulation 1049/2001, and EUCI documents are subject to specific rules, defined in Article 9 of Regulation 1049/2001[36].

---

[32] Article 9 ('Treatment of sensitive documents') provides, amongst others, for prior declassification of the documents before access can be granted.

[33] Subject to the conditions defined in its Article 9 ('Treatment of sensitive documents'), which provides, amongst others, for prior declassification of the documents before access can be granted.

[34] Annex II - Forwarding of confidential information to the European Parliament.

[35] In accordance with Articles 3 and 4 of the Detailed Rules of Application of Regulation 1049/2001 (Official Journal L 345 of 29 December 2001, p. 94), without prejudice to the procedural requirements defined in Article 9 of Regulation 1049/2001 in case of classified documents.

[36] See the explanatory fiche on access to classified and marked documents: https://myintracomm.ec.europa.eu/sg/docinter/Documents/Fiche_12_classified_documents.pdf.

4.5. Reporting unauthorised disclosure

Unauthorised disclosure of information must be reported to HR.DS. This is especially the case for any information at SNC level and above.

A witness of an unauthorised disclosure/information leak should report the leak directly and immediately to HR.DS.

Unauthorised disclosure of personal data must also be reported, without undue delay, to the DPO.

4.6. Reporting information security incidents

In case any defects or breaches are observed in the protection of information in an IT system, these must be reported to the local IT service desk, which should report them to the Local Informatics Security Officer (LISO), the Local Security Officer (LSO) and, in the case of an information security breach, to HR.DS, and in case of a personal data breach to the Data Protection Officer.

IT security incidents must additionally be reported in line with the relevant procedures defined under Decision 2017/46.