EUROPEAN
COMMISSION

Brussels, 5.3.2019
C(2019) 1904 final

Security Notice

Marking and handling of sensitive non-classified information

Contents

1. INTRODUCTION

1.1. Key elements

Commission staff must mark sensitive non-classified information in line with this security notice.

The purpose of marking information is to ensure a sufficient level of confidentiality for the information. Markings are based on the fundamental security principles of **need-to-know.** A marking consists of a security marking plus any distribution markings, as described in this document. Marked information must be protected adequately in information systems, where possible by using encryption.

The two possible security markings are SENSITIVE and SPECIAL HANDLING. Each of these indicates that the information is sensitive non-classified. Documents marked as **SENSITIVE** are handled in accordance with the standard handling instructions below. **SPECIAL HANDLING** indicates that specific, stricter handling instructions apply. **The distribution marking provides information on the need-to-know for the information.**

Rules for EU classified information (EUCI) are given in the relevant implementing rules under Commission Decision (EU, Euratom) 2015/444[1], and are outside the scope of this security notice. Less sensitive information, at the levels Commission Use (CU) and Publicly Available (PA), does not need to be marked.

1.2. Legal basis

The legal basis for security markings is laid out in Commission Decision (EU, Euratom) 2015/443[2], in particular Article 9. This Decision covers the security of persons, physical assets and information.

Article 9(6) of Commission Decision (EU, Euratom) 2015/443 states that '(…) *When deemed necessary for the effective protection of its confidentiality, [Sensitive non-classified information] shall be identified by a security marking and corresponding handling instructions approved by the Director-General for Human Resources and Security*.'

Sensitive non-classified (SNC) information is the information whose unauthorised disclosure could cause damage to the Commission or other interested parties such as businesses, companies, intellectual property or personal data but which is not EU classified information. It is defined in Commission Decision (EU, Euratom) 2015/443 as '*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*'. This

[1] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (Official Journal L 72 of 17 March 2015, p. 53)

[2] 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)

information is covered by the obligations of confidentiality established in Article 339 of the Treaty on the Functioning of the European Union (TFEU) and in Article 17 of the Staff Regulations.

Without prejudice to the above, any document held by the Commission, including documents containing sensitive information, may be subject to a request for public access to documents and must be assessed pursuant to Regulation 1049/2001[3] in light of the factual and legal circumstances that apply at the time of the adoption of the decision on access[4].

Without prejudice to the above, any personal data stored in such documents (or otherwise processed) by the Commission may be subject to requests from the data subjects whose personal data are processed. Such requests must be assessed pursuant to Regulation (EU) 2018/1725[5].

1.3. Further information

Any queries on this security notice should be addressed to the functional mailbox HR MAIL DS3. For any inquiry concerning the applicable procedures within a particular DG, the local security officer should be contacted.

2. SECURITY MARKINGS

2.1. Commission Markings

There are two security markings for SNC information, which are **SENSITIVE** and **SPECIAL HANDLING**. **SENSITIVE** indicates that the standard handling instructions given below must be applied. **SPECIAL HANDLING** indicates that specific handling instructions apply, which must be available for consultation. The **SPECIAL HANDLING** security marking is not applicable Commission-wide (see section 5.2 and Annex 3 below).

The handling instructions address all stages of the lifecycle of a document or information asset, which are creation, handling (i.e. reading editing or storing), copying, distribution, downgrading and destruction. There are specific instructions, where relevant, for the handling of physical documents and electronic documents.

Security markings may be applied to individual documents or to collections of documents, such as those managed in document management systems or physical

---

3 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 145 of 31 May 2001, p. 43).

4 For details on the handling of marked documents in case of an application for access to documents, please see the explanatory fiche on access to classified and marked documents: https://myintracomm.ec.europa.eu/sg/docinter/Documents/Fiche_12_classified_documents.pdf.

5 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.

document stores[6]. In particular, when large quantities of documents are obtained from third parties, it may be appropriate to mark the document store rather than each individual document[7].

Further information should be given by one or more distribution markings as described in the next section.

Previously existing security markings on sensitive non-classified documents do not need to be replaced. However, they must be handled in line with this document, based on the equivalent new marking in the conversion table in Annex 1.

2.2. Interinstitutional markings

When exchanging non-classified documents with other EU institutions, their internal markings may be used to ensure the proper handling of the documents by the recipients. In particular, the 'Limité/Limited' marking of the Council may be used which restricts distribution to the EU institutions, EU member states and EEA states. Documents bearing this marking should be marked as **SENSITIVE** inside the Commission.

3. DISTRIBUTION MARKINGS

The security marking **SENSITIVE** may be used on its own or with one or more distribution markings to help users to determine whether they have a need-to-know for the document.

When **SENSITIVE** is used on its own, the target audience is not predefined and the originator can therefore distribute the information according to the business need. Recipients may share the information within the Commission to personnel with a need-to-know[8].

The distribution markings indicate restrictions on the authorised recipients or the expected timeframe of the sensitivity of a document, since some documents are only sensitive until a certain date or event.

A number of distribution markings (or 'reserved distribution markings') are defined in Annex 2. These markings cover some of the Commission's core administrative activities and may only be used in accordance with the restrictions given.

Some distribution markings, such as *Staff matter*, imply that the contents include data covered by the Data Protection Regulation. This regulation is applicable to all documents containing personal information, irrespective of the marking.

---

6 A document store may be a physical container such as a file, box or cupboard, or an electronic repository such as a shared folder or a database.

7 Nevertheless, if individual documents are taken out of the store, they must be marked appropriately.

8 This includes staff handling applications for public access to documents under Regulation 1049/2001 in the Commission's Secretariat-General, in accordance with Article 4 of the Detailed Rules of Application of Regulation 1049/2001, Official Journal L 345 of 29 December 2001, p. 94.

Any distribution marking indicating the authorised recipients, whether by organisation or subject matter, must be included together with the main security marking, separated by a colon. This will be one of the following options:

- A reserved distribution marking;
- The abbreviated name of one or more DGs or services; or
- An agreed workgroup name or other designation.

A reserved distribution marking, as given in Annex 3, must be used with the security marking **SPECIAL HANDLING**.

Other distribution markings, either indicating deadlines or TLP[9] markings, may be included on the same line or on a second line below the main security marking. The available distribution markings are explained below.

Annex 1 shows all of the markings from the former Security Notice 1 on the use and application of markings, and their equivalents under the current scheme.

3.1. Reserved distribution markings

The list of reserved distribution markings and the restrictions on their use is given in Annex 2 and Annex 3.

3.2. Abbreviated names

Instead of one of the predefined markings, the distribution marking may include a definition of the target audience or authorised recipients. This may take one of the following forms:

- DG [DG name], e.g. 'DG HR';
- DG [DG name].[Directorate], e.g. 'DG HR.DS';
- DG [DG name].[Directorate].[Unit], e.g. 'DG HR.DS.3'.

Multiple entities may be specified, separated by commas. Commission departments must always be specified using their standard abbreviations (e.g. HR, DIGIT, SG …).

3.3. Working groups or other designations

Group names may be defined for specific topics or for working groups that have a clearly defined membership, particularly when the group includes members from multiple DGs or from outside the Commission. The membership of the group must always be traceable to ensure that the authorised recipients are known and to assist with the investigation of any leaks.

[9] Traffic Light Protocol; a common marking scheme that may be used when communicating with third parties. See below paragraph 3.4.3

Consequently, **group names must be formally defined and agreed between the leading DG of a working group and its LSO and the document management officer (DMO)**. The LSO must keep a record of all group names created by the department and must inform HR.DS of any changes by email to HR MAIL DS3.

When this option is used, the document may be shared within the defined audience. While some flexibility in sharing such documents within the Commission may be allowed where there is a business need, they must not be shared with third parties without authorisation from the originator[10].

3.4. Other distribution markings

The following additional distribution markings are optional and, when used, may be included in the first line or as a second line below the main security marking.

3.4.1. Date markings

The markings *UNTIL xx/xx/xxxx* and *EMBARGO UNTIL xx/xx/xxxx* are intended to indicate time restrictions on applicability of the marking. *EMBARGO UNTIL* indicates a temporary block on the availability of information to third parties or in communication and information systems (CISs)

These markings may be used with or without another distribution marking.

When applied to a document which might only be made available at a later, as yet unknown date, the embargo could be unlimited e.g. *EMBARGO (UNLIMITED).*

3.4.2. Releasability markings

The marking *RELEASABLE TO* **…** is used to indicate that the document may be given to a particular organisation or third party even if other handling restrictions might remain in place.

Examples:

RELEASABLE TO: EUROPEAN PARLIAMENT

RELEASABLE TO: CROATIA

RELEASABLE TO: EU AND EEA MEMBER STATES

RELEASABLE TO: EU INSTITUTIONS, EU MEMBER STATES, and EEA STATES[11]

There should be a clear understanding of which groups or persons within the named organisation or third party are authorised to receive the document.

---

[10] The originator in this case refers to the service that bears the legal responsibility for protecting the document or information within the European Commission.

[11] Note that this is the scope of the present 'Limité' marking that is used between the EU institutions, but the handling instructions may be different.

Where a country name is specified, this only implies that the information is releasable to the relevant service of the national administration. An agreement to exchange sensitive information must be in place with any third country identified as the recipient of the information.

3.4.3. TLP markings

The Traffic Light Protocol[12] markings *TLP AMBER* and *TLP RED* may be used in combination with the security marking. TLP markings are only to be used for the purpose of facilitating exchanges of information with third parties, and have no validity within the Commission. They must not be implemented in corporate CISs.

Generally, *TLP AMBER* will correspond to **SENSITIVE** and *TLP RED* will correspond to **SPECIAL HANDLING**. The colour codes foreseen for TLP can be used if necessary.

Examples:

SENSITIVE: *TLP: AMBER*

SENSITIVE: *TLP: AMBER*

4. APPLICATION OF MARKINGS

4.1. Markings in documents

The main security marking (**SENSITIVE** or **SPECIAL HANDLING**) must be in Times New Roman, font size 14, bold, and in capital letters. Distribution markings must follow a colon and be in Times New Roman, 14, italics, as given in this document, e.g. '*Security matter*'.

In text documents (e.g. Word documents), whether in paper or digital form, the markings must be indicated on the top right side of the front page of the document, under the reference number of the document where applicable (see the example below and the sample documents in Annexes 4 and 5). In other types of documents (e.g. Excel or PowerPoint documents), the marking must be positioned in a similar position on the first printed page.

Distribution markings must be placed on the same line, and may also continue on a second line if there is insufficient space on one line (the marking should not extend past the centre of the page).

SENSITIVE: *Security matter*
UNTIL 31/12/2018

In the above example, the main security marking is **SENSITIVE**, and the distribution marking '*Security matter*' indicates the restrictions based on the

[12] See https://www.first.org/tlp/ for the definitions of the levels and further information.

subject matter. After the deadline, the document is no longer considered as sensitive non-classified information (by default, it will then revert to the next lower level, 'Commission Use').

The main security marking may also be included in the header of a document on each subsequent page. In this case, it must be included in normal text at the standard font size of the header, on the right side of the header (see Annex 5).

The use of watermarks or headers such as 'CONFIDENTIAL' or 'RESTRICTED' or any other indication of confidentiality is prohibited.

Draft documents can be marked, and a watermark may indicate that the document is a draft (this is not a security marking).

4.2. Markings in communication and information systems (CISs)

4.2.1. Email

Users should mark emails containing SNC information. The subject line should not contain SNC information. The first line of the email, before any salutation or other text, should include all markings and other instructions, on one line and separated by dashes. The main security markings should be in bold and the distribution markings in italics, and not smaller than the main text, as in the example below (see also the sample email in Annex 6):

> **SENSITIVE:** *Security matter*
>
> Dear colleague,
>
> I enclose the list of candidates for the post of …[etc.]
>
> …

In accordance with the handling instructions in Section 5 below, all SNC emails must be signed and encrypted using SECEM[13] or equivalent encryption products.

In line with the established practices across the Commission, secure emails should be handled as **SENSITIVE**, even when not marked.

4.2.2. Web-based CISs

It is recommended that CISs implemented with web interfaces display the appropriate marking on all screens that may contain SNC information. As an example, the marking should appear towards the top right of the screen, and should include a link to the relevant handling instructions.

All printouts containing SNC information must bear the appropriate markings.

---

[13] SECEM (SECure EMail) is the function in Outlook that enables users to encrypt and sign emails, based on the S/MIME standard. To obtain the certificate necessary for using SECEM, visit the CommisSign-2 web page at http://commissign.pki.ec.europa.eu/index_en.htm.

4.2.3. Document handling systems

Document handling systems must clearly indicate any security markings applied to the document before it is opened, as well as in the document itself as described in Sections 4.1 and 4.2 above. See Section 6.2 below for instructions on document metadata.

Further information on the implementation of security markings in individual systems must be provided by the system owner. HR.DS can provide advice on this subject upon request.

The principles of need-to-know and the handling instructions for security markings must be implemented in the rules defined in the CIS's access control policy and automated as far as possible in the CIS.

4.2.4. Other CISs

When all of the information in a CIS is SNC, the recommended approach for CISs that handle SNC is to present a warning screen to the user when entering the system. This may be shown on the authentication screen or as a separate message after authentication.

The warning screen should clearly show all markings (the main security marking and any distribution markings). The warning screen should show the handling instructions that relate to the system or output from the system (e.g. printouts), or include a link to those instructions. A link to the acceptable use policy of the system may also be included.

When the CIS contains both SNC and non-sensitive information, any SNC information should be clearly marked on screen before the user can access the contents.

All printouts containing SNC information must bear the appropriate markings.

HR.DS.3 can provide support to CIS owners when implementing markings in their system.

5. HANDLING INSTRUCTIONS

5.1. SENSITIVE

The standard handling instructions apply to all documents bearing the marking **SENSITIVE**.

Where necessary, mandated staff[14] may specify additional handling instructions.

[14] Under Article 5 of Commission Decision (EU, Euratom) 2015/443 or Regulation (EU, Euratom) 2016/2030 amending Regulation (EU, Euratom) 883/2013, as regards the secretariat of the Supervisory Committee of the European Anti-Fraud Office (OLAF) (Official Journal L 317 of 23 November 2016, p. 1).

Creation

Creation covers any restrictions on the drafting of a document or the creation of information. Generally, there are no restrictions on the creation of documents at the SNC level, although the use of CISs containing functions for automatically adding markings in the correct formats is recommended.

The author of a document must select the appropriate distribution marking, based on the subject matter and the level of damage that may be caused by unauthorised disclosure.

Each document bearing the marking **SENSITIVE** must include either:

- a footnote with a link to the standard handling instructions (optionally including a summary of the main handling instructions), or
- the handling instructions themselves.

Handling

Handling includes the instructions for reading, editing, copying, scanning, printing and storing documents.

Recipients may further distribute the information on a need-to-know basis, bearing in mind the principle of professional secrecy and the obligations under the Staff Regulations (Article 17). However, recipients must be aware that the document must not be released outside the EU institutions and Member States' public administrations without permission from the originator.

Care should be taken not to leave documents unattended on office desks. Where possible, documents should be stored in a locked office or a locked cupboard when not in use.

Documents should not be read or edited in public places where there is a risk of them being read by unauthorised people.

Electronic copies should be stored on platforms that can only be accessed by the target audience. The use of encryption and digital signatures is recommended, taking into account the risks and other countermeasures in place.

Scanned copies of documents, including both electronic and hard copies, should be removed from any insufficiently secured locations as soon as possible, including shared drives, unencrypted emails, scanner device memory and printers in unsecured office areas.

Documents should be removed from printers, photocopiers, faxes or other shared devices immediately. Care should be taken to limit the number of copies to the minimum necessary.

Distribution

Distribution covers the definition of the authorised recipients, methods of transmitting the information to those recipients (including carriage and electronic transmission) and the rules to be followed by the recipients, with particular regard to the further distribution by recipients. Distribution also includes any restrictions on translation.

Distribution is on a need-to-know basis, and the information is not to be distributed outside of the audience indicated.

All recipients should be aware of the applicable handling instructions.

Any person receiving SNC information who is not the intended recipient must inform the sender, where possible, and destroy the information by appropriate secure procedures (see under 'Destruction' below).

Where internal mail is used, the information must be closed[15] inside an opaque envelope.

Where email is used to transmit SNC information, even partially, the use of the SECEM application (or similar) is mandatory, i.e. the emails must be signed and encrypted.

Downgrading

When a document no longer needs to be marked, the markings and handling instructions should be removed or struck out. Only the originator may downgrade a document.

Destruction

Paper documents must be shredded using at least a German DIN standard 66399 level 3 shredder (straight cut 1.9 or cross cut 4 x 80 mm, max 320 mm2)[16]. Shredded documents may be disposed of in the normal office waste.

Documents stored on electronic media must be purged[17]. If the media is not to be reused, they must be disposed of in line with the *Standard on Sanitisation of Media*[18].

---

[15] In this context, 'closed' indicates that an envelope has been closed in a way that makes it evident that the contents may have been accessed, whether deliberately or accidentally. This includes gluing or stapling the flap of the envelope closed; it does not require the use of a specific seal or stamp.

[16] This instruction is without prejudice to the provisions of Commission Decision 2002/47/EC, ECSC, Euratom on document management (Official Journal L 251 of 27 February 2004, p. 9) and Commission Decision 2004/563/EC, Euratom on electronic and digitised documents (Official Journal L 282 of 19 October 2016, p. 19).

[17] The method of purging depends on the type of medium as follows:
- Magnetic tapes — degaussing;
- Magnetic disks — degaussing or overwriting with approved software;
- Flash memory (USB keys, SD cards, SSD drives, etc.) — overwriting with approved software;

5.2. SPECIAL HANDLING

This security marking indicates that more specific handling instructions apply to the document, as indicated by the distribution marking. The handling instructions for **SPECIAL HANDLING** are based on those defined for **SENSITIVE** in Section 5.1[19] plus the additional instructions below.

The **SPECIAL HANDLING** marking may only be applied within the security environment of the originating department or by other parties under a memorandum of understanding that they will apply equivalent security measures. Users of the **SPECIAL HANDLING** marking should be aware that it is not supported in many of the corporate systems.

The document must contain either the relevant handling instructions or a link to indicate where the user can consult the instructions. The recommended approach is to implement this in a footnote to the marking, as shown below:

SPECIAL HANDLING: *ETS Critical*[1]

[1]Handling instructions are given at https://www.europa.eu/handling_instructions

Distribution markings under **SPECIAL HANDLING** and their associated handling instructions must be submitted to the Security Directorate of DG HR for approval and inclusion in this document before use. See Annex 3 for the approved **SPECIAL HANDLING** markings and a summary of the related handling instructions.

The recommended additional handling instructions for SPECIAL HANDLING are given below. Each SPECIAL HANDLING distribution marking may also include specific instructions based on the business need (given in Annex 3). If the security needs require significantly stricter handling instructions, then the originator is advised to consider classifying the information as EUCI.

Creation

Restrictions will apply to the services that are permitted to use a **SPECIAL HANDLING** marking, as defined in Annex 3.

There may be restrictions on the environments where such documents may be created, e.g. only on a specified CIS.

- Non-rewriteable media (optical disks, non-volatile solid state devices, smart cards …) — physical destruction.

[18] https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Documents/ST_sanitisation.doc

[19] Unless they are superseded by the **SPECIAL HANDLING** instructions.

Handling

Recipients may not distribute documents without explicit permission from the originator[20].

Documents must not be read or edited in public places where there is a risk of them being seen.

Documents must be stored in a locked office or in a locked cupboard or safe. Electronic copies should be stored on platforms that can only be accessed by the target audience. The use of encryption and digital signatures should be considered, taking into account the risks and other countermeasures in place.

The originator may direct that documents must not be stored in document handling systems but only the metadata (document title, originator, reference number …) may be registered there. The metadata, including the document title, should not reveal SNC information.

Printing, copying and scanning must be performed on appropriately secured devices.

Outside Commission premises, documents must be carried in an opaque container (envelope, briefcase etc.).

Distribution

Distribution is on a strict need-to-know basis, and the information is not to be distributed outside of the audience indicated.

Recipients must obtain permission from the originator before distributing to other parties[21].

Where internal mail is used, the information must be sealed inside an opaque envelope and accompanied by the relevant handling instructions. When the document must only be accessed by the named recipient, it must be sent inside a double sealed envelope with the text "RECIPIENT ONLY" on the inner envelope.

Emails must be digitally signed and encrypted.

Translation may only take place on Commission premises, without any outsourcing.

---

[20] Except where this conflicts with Regulation 1049/2001 and the administrative arrangements defined in Article 4 of the Detailed Rules of application of the regulation (Official Journal L 345 of 29 December 2001, p. 94). In accordance with Article 6(e) of Commission Decision (2008/597/EC), the Data Protection Officer should have access at all times to the data forming the subject matter of processing operations on personal data and to all offices, data-processing installations and data carriers.

[21] Except where this conflicts with Regulation 1049/2001 and the administrative arrangements defined in Article 4 of the Detailed Rules of application of the regulation (Official Journal L 345 of 29 December 2001, p. 94), and except where it conflicts with Regulation (EU) 2018/1725.

Downgrading

Instructions on the conditions for downgrading documents should be defined in the handling instructions, based on the business requirements. Only the originator may decide on the downgrading of a document.

Destruction

Paper documents must be shredded using at least a German DIN standard 66399 level 4 shredder (cross cut 2 x 15 mm, max 160 mm2)[22]. Shredded documents may be disposed of in the normal office waste.

6. OTHER ISSUES

6.1. Personal Information

Documents with certain distribution markings will, by their nature, contain personal information but may only be initiated by specific services. In some cases, the human resources responsible and the management of a department may also need access to these documents (*Staff matter*, *Medical secret*, *Investigations and disciplinary matters*, *Mediation service matter*, *Opinion of the legal service* and in some cases *Security matter*).

Personal information must be handled in line with Regulation (EU) 2018/1725. The Data Protection Officer should have access at all times to the data forming the subject matter of processing operations on personal data and to all offices, data-processing installations and data carriers. Duly authorised staff in Commission departments, who handle requests of individuals for access to their personal data or for the exercise of their other rights under Regulation (EU) 2018/1725, also need to be able to access Commission documents containing personal data

6.2. Archiving and Access to Documents

While performing their duties, Document Management Officers (DMOs) or Historical Archives Service staff might need to handle documents with markings and to access SNC information, for instance when the originator of a document cannot be identified. In such cases the DMO of the service holding the document might be authorized to access specific sensitive contents and shall determine the actions required with a view to ensure the confidentiality of information[23].

The Commission's Common Retention List[24] gives a schedule for the retention of different types of documents.

---

[22] This instruction is without prejudice to the provisions of Commission Decision 2002/47/EC, ECSC, Euratom on document management (Official Journal L 251 of 27 February 2004, p. 9) and Commission Decision 2004/563/EC, Euratom on electronic and digitised documents (Official Journal L 282 of 19 October 2016, p. 19).

[23] For instance giving access to involved stakeholders as per hierarchy's request

[24] See Ares(2012)1501883 First revision of the Commission's common retention list

The rules for the handling of marked documents are to be applied without prejudice to the Regulation 1049/2001 and its Detailed Rules of Application, the Framework Agreement on relations between the European Parliament and the Commission[25], and the principle of sincere cooperation with the Member States. Any document held by the Commission, including documents containing sensitive information, may be subject to a request for public access to documents and must be assessed pursuant to Regulation 1049/2001 in light of the factual and legal circumstances that apply at the time of the adoption of the decision on access. Staff handling applications for access to documents under Regulation 1049/2001 in Commission Directorates-General and services and in the Secretariat-General also need to be able to access Commission documents forming the subject of applications for public access.

For details on the handling of marked documents in case of an application for access to documents, please see the explanatory fiche on access to classified and marked documents:

https://myintracomm.ec.europa.eu/sg/docinter/Documents/Fiche_12_classified_documents.pdf.

6.3. Markings in document metadata

Document handling systems often record metadata about the documents, which contain information such as the title, author, creation date, etc. of the document. Where a system records metadata, this must also include the security markings to enable the system to display the markings to users and to transfer documents to other systems and ensure consistent handling.

Each document should include a property named 'Security marking' which will contain the marking, i.e. either 'SENSITIVE' or 'SPECIAL HANDLING'.

Other properties may be included for the distribution markings.

6.4. Translation

When documents bearing a security marking need to be translated, the workflow and any associated systems must take account of the markings. In particular:

- The principles of need-to-know must be applied;
- Translators must be aware of and follow the handling instructions;
- Marked documents must be encrypted when transmitted electronically;
- Systems used by translators must follow the instructions in Section 6.1 above;

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

- Marked documents and translations must be securely deleted[26] from non-Commission systems when the translation has been completed.

6.5. Use of markings with external partners

In certain circumstances it might be necessary for a service to exchange information with one or more third parties outside the Commission.

As a marking is only legally enforceable within the Commission, a memorandum of understanding, contract or security convention should be drawn up between the Commission DG/service and the external party, setting out the handling instructions for all information exchanged between them. This is done on the basis of trust, and each entity is responsible for the compliance by its own staff handling the information exchanged.

The appropriate handling instructions must be included with any document bearing a marking that is shared with third parties.

HR.DS can provide assistance on this topic upon request.

6.6. Exceptions for mandated staff

Sensitive non-classified information may be accessed by Commission staff with an appropriate legal mandate in the context of internal investigations or audits, or for business continuity purposes.

[26] Secure deletion ensures that the contents of a file are overwritten in the storage media (hard disk, etc.), leaving no traces of the file.

ANNEX 1: CONVERSION TABLE

The table below shows the equivalent new marking for all of the markings from the previous version of this security notice. A number of distribution markings are reserved for specific services and may not be used by others.

Previous marking	**New marking**
Commission internal	**[No equivalent]**[27]
Limited	**[No equivalent]**[28]
Limited DG	**SENSITIVE**: *DG xxx + …*
Limited Service/Unit/Group	**SENSITIVE**: *[group name]*
Personal	[No equivalent]
Personal data	[No equivalent][29]
Embargo until	See Section 3.4.1
Deadline	See Section 3.4.1
RELEASABLE TO	See Section 3.4.2
Investigations and disciplinary matters	**SENSITIVE**: *Investigations and disciplinary matters*
OLAF Investigations	**SENSITIVE**: *OLAF Investigations*
OLAF Investigations — Special handling	**SPECIAL HANDLING**: *OLAF Investigations*
Mediation Service Matter	**SENSITIVE**: *Mediation service*
Staff matter	**SENSITIVE**: *Staff matter*
COMP Operations	**SENSITIVE**: *COMP Operations*
COMP — Special handling	**SPECIAL HANDLING**: *COMP*

[27] The security marking **SENSITIVE** on its own is the closest match to Commission Internal but the definition is slightly different (see Section 3). The most appropriate marking in the present scheme must be selected.

[28] In cases where the previous Limited marking of the Commission would be applied, the most appropriate marking in the present scheme must be selected. Documents bearing a 'Limité/Limited' marking of another EU institution should also be marked as **SENSITIVE** inside the Commission.

[29] See the guidance issued by the European Data Protection Supervisor. Personal data should generally be considered as sensitive non-classified and marked, in which case the most relevant marking must be applied in accordance with this security notice.

Previous marking	**New marking**
Medical secret	**SENSITIVE**: *Medical secret*
Opinion of the Legal Service	**SENSITIVE**: *Opinion of the Legal Service*
Court procedural documents	**SENSITIVE**: *Court procedural documents*
Security matter	**SENSITIVE**: *Security matter*
ETS Limited	**SENSITIVE**: *ETS Joint Procurement*
ETS Sensitive	**SENSITIVE**: ETS
ETS Critical	**SPECIAL HANDLING:** *ETS Critical*
EU satellite navigation matter	[No equivalent]
Pharma investigations	**SENSITIVE**: *Pharma investigations*
Pharma investigations — special handling	**SPECIAL HANDLING**: *Pharma investigations*
IAS OPERATIONS	**SENSITIVE:** *IAS operations*
Economy and finance	**SPECIAL HANDLING:** *Economy and finance*

ANNEX 2: RESERVED DISTRIBUTION MARKINGS — SENSITIVE

The table below lists all of the reserved distribution markings that may be used with the security marking **SENSITIVE**, with details of the restrictions on their use.

Distribution marking	**Restrictions**
COMP Operations	Only to be applied by DG COMP.
Court procedural documents	Only to be applied by the Legal Service of the Commission.
Opinion of the Legal Service	Only to be applied by the Legal Service of the Commission.
CLIMA	Only to be applied by DG CLIMA.
IAS Operations	Only to be applied by the IAS.
Investigations and disciplinary matters	For information processed by the Investigation and Disciplinary Office of the Commission. Everybody must apply this marking when dealing with information processed by IDOC.
Mediation Service	Only to be applied by the Mediation Service, the Director and Heads of Unit of the PMO, the Director-General, Director and Heads of Unit of DG HR, the Director-General of the Legal Service and the Resources Directors.
Medical Secret	Only to be applied by the Medical Service (DG HR), the joint sickness insurance service (PMO). Covered by medical confidentiality rules.
OLAF Investigations	For information processed by the European Anti-Fraud Office (OLAF). Everybody must apply this marking when dealing with information processed by OLAF.
Pharma investigations	Only to be applied by DG SANTE.
Staff matter	To be used only for documents related to active or former staff matters and managed by staff of personnel departments and management concerned, and to be opened by the addressee(s).

Distribution marking	**Restrictions**
Security matter	Only to be initiated by HR DS and ECHO security services.

ANNEX 3: DISTRIBUTION MARKINGS — SPECIAL HANDLING

The distribution markings that are defined for use under SPECIAL HANDLING are reserved for specific services and business purposes and may not be used by others. The associated handling instructions are only valid within the originating DG.

The SPECIAL HANDLING distribution markings and associated full handling instructions are available on MyIntracomm[30].

The table below lists all of these distribution markings with details of the restrictions on their use.

Distribution marking	**Restrictions**	**Further information**
COMP	Only to be initiated by DG COMP	Upgraded marking for more sensitive documents applied within the marking scheme for DG COMP Antitrust, Mergers, State Aid and other proceedings. This marking is applied in rather exceptional circumstances to a limited number of documents. Full handling instructions are provided by DG COMP.
Economy and finance	This marking may only be initiated by DG ECFIN, 'Task Forces' or other services linked to DG ECFIN on instruction from the hierarchy at the level of Director	Marking to be applied on documents which contain SNC information on economic and financial matters. Full handling instructions are provided by DG ECFIN.
CLIMA	Documents may only be distributed to and the marking only be used by persons listed in the ETS critical authorised users list kept by DG CLIMA	Marking to be applied to highly sensitive Emission Trading Scheme (ETS) operational information defined in the ETS sensitive information list maintained by DG CLIMA. Full handling instructions are provided by DG CLIMA.

[30] See https://myintracomm.ec.europa.eu/corp/security/EN/newDS3/SensitiveInformation/Pages/protective-marking-system.aspx

Distribution marking	Restrictions	Further information
OLAF investigations	Only to be used by OLAF	For information processed by the European Anti-Fraud Office (OLAF). Full handling instructions are provided by OLAF.
Pharma investigations	Only to be initiated by DG SANTE	Upgraded marking for more sensitive documents applied within the marking scheme for DG SANTE penalty proceedings. This marking is applied in rather exceptional circumstances to a limited number of documents. Full handling instructions are provided by DG SANTE.

ANNEX 4: SAMPLE MARKED NOTE

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY

Directorate HR.DS - Security

HR.DS.3

SENSITIVE[1]: *Security matter*

NOTE ON THE SECURITY PROCEDURES OF THE COMMISSION

Subject: **Example markings**

This note includes an example of the marking for security matters.

Director, HR.DS

[1] Handling instructions for SENSITIVE information are given at https://ec.europa.eu/handling_instructions

ANNEX 5: SAMPLE MARKED REPORT (FIRST AND SECOND PAGES)

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
DS3 Information Security

HR.DS.3

SENSITIVE[1]: *Security matter*
Deadline: 31 March 2018

Report on the Security Procedures of the Commission

Final version, 19 January 2018

[1] Handling instructions for SENSITIVE information are given at https://ec.europa.eu/handling_instructions

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111

Table of Contents

ANNEX 6: SAMPLE EMAIL