

2019-208

Adopted on 30.08.2019

Decision of the Management Board on the Security Rules for Protecting Sensitive Non-classified Information at eu-LISA

Handling instructions for the marking LIMITED BASIC

- Distribution on a need-to-know basis.
- Not to be released outside of the information stakeholders.
- Not for publication.

The Management Board,

Having regard to Regulation (EU) 2018/1726 of the European Parliament and the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011¹,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission²,

Having regard to Commission Security Notice of 5 March 2019 on marking and handling of sensitive non-classified information³,

Having regard to Decision of the Management Board on Security Rules in eu-LISA 2016-133 REV 3⁴,

WHEREAS:

- (1) In accordance with Article 37(1) of Regulation (EU) 2018/1726, eu-LISA shall adopt its own security rules on sensitive non-classified information based on the principles and rules laid down in Commission Decision (EU, Euratom) 2015/443.
- (2) The Commission adopted on 5 March 2019 the Security Notice on marking and handling of sensitive non-classified information, based on Commission Decision (EU, Euratom) 2015/443, and therefore the Agency's rules should also be based on that Security Notice.
- (3) Under Article 14(6) of Decision of the Management Board on Security Rules in eu-LISA 2016-133 REV 3, sensitive non-classified information shall be subject to rules regarding its handling and storage and shall only be released to those individuals who have a need to know. Where deemed necessary for the effective

¹ OJ L 295, 21.11.2018, p.99.

² OJ L 72, 17.3.2015, p.41.

³ C(2019) 1904 final.

⁴ Decision of the Management Board on Security Rules in eu-LISA 2016-133 REV3 adopted on 27.07.2017.

protection of its confidentiality, it shall be identified by a security marking and corresponding handling instructions.

- (4) In accordance with Article 37(2) of Regulation (EU) 2018/1726, security rules of eu-LISA for protecting sensitive non-classified information shall be adopted by the Management Board of eu-LISA following approval by the Commission.
- (5) It is important that, where appropriate, all the EU institutions, agencies, bodies or offices, are associated with the principles, standards and rules for protecting sensitive non-classified information which are necessary in order to protect the interests of the Union and its Member States.
- (6) The security measures taken according to this Decision should be compliant with the principles for security in the Decision of the Management Board on Security Rules in eu-LISA 2016-133 REV 3, including the principles of legality, transparency, proportionality and accountability,

Has adopted the following Decision:

Contents

Chapter 1	GENERAL PRINCIPLES	1
Article 1	Subject matter and scope	1
Article 2	Marking SNC information	1
Article 3	Security marking	2
Article 4	Interinstitutional markings	2
Article 5	Distribution markings.....	2
Chapter 2	APPLICATION OF MARKING	5
Article 6	Markings in documents	5
Article 7	Markings in communication and information systems (CISs).....	6
Article 8	Markings in document metadata.....	7
Chapter 3	HANDLING INSTRUCTION FOR SNC INFORMATION.....	7
Article 9	Handling instructions for SNC information marked SENSITIVE	7
Chapter 4	OTHER ISSUES	10
Article 10	Personal information	10
Article 11	Archiving and access to documents	10
Article 12	Translation	11
Article 13	Use of markings with external partners.....	11
Article 14	Exceptions for mandated staff	11
Article 15	Entry into force	11
Annex 1:	CONVERSION TABLE	12
Annex 2:	RESERVED DISTRIBUTION MARKINGS	13

Chapter 1 GENERAL PRINCIPLES

Article 1 Subject matter and scope

1. This Decision lays down the rules, basic principles and minimum standards for the protection of sensitive non-classified information in eu-LISA ('SNC information'), including its handling marking and storage.
2. For the purpose of this document, SNC information *is information or material eu-LISA must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity*⁵. SNC information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No. 1049/2001 of the European Parliament and of the Council⁶ read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EU) 2018/1725 of the European Parliament and of the Council⁷.
3. This Decision shall apply to all eu-LISA departments and in all premises of eu-LISA.
4. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to the Members of the Management Board and of Advisory Groups, to eu-LISA staff under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Communities, to national experts seconded to eu-LISA (SNEs), to service providers and their staff, to interns and to any individual with access to eu-LISA buildings or other assets, or to information handled by eu-LISA.
5. Rules for handling EU classified information (EUCI) are outside the scope of this document.

Article 2 Marking SNC information

1. eu-LISA staff must mark sensitive non-classified information in line with the present security rules.

⁵ In line with art.14.5b) of Management Board Decision on Security Rules in eu-LISA, 2016-133 REV3.

⁶ 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 (OJ L 145, 31.5.2001, p.43).

⁷ Regulation (EU) No 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 (OJ L 295, 21.11.2018, p.39).

2. The purpose of marking information is to ensure a sufficient level of protection for the information. Markings are based on the fundamental security principle of 'need-to-know'.
3. Markings for SNC information are divided in two categories: security marking and distribution markings.
 - a. Security marking defines the level of security and the corresponding restrictions to access to this information.
 - b. Distribution markings indicate restrictions on the authorised recipients or the expected timeframe of the sensitivity of a document.

Article 3 Security marking

1. The security marking for SNC information in eu-LISA is "SENSITIVE" based on the following assessment: any information reserved for a limited number of persons on a need to know or need to access principle and whose disclosure to unauthorised persons would cause moderate prejudice to eu-LISA, the EU institutions and bodies, Member States or other parties, but not to an extent serious enough to merit EU classification.
2. All SNC information in eu-LISA shall carry one security marking.
3. Security markings may be applied to individual documents or to collections of documents, such as those managed in document management systems or physical document stores⁸. When large quantities of documents are obtained from third parties, it is allowed to mark the document store rather than each individual document. Nevertheless, if individual documents are taken out of the store, they must be marked appropriately.

Article 4 Interinstitutional markings

When exchanging non-classified documents with EU institutions and Member States, their internal markings may be used to ensure the proper handling of the documents by the recipients. Documents bearing such marking shall be handled as **SENSITIVE** in eu-LISA.

Article 5 Distribution markings

General aspects

1. Distribution markings may be applied to indicate to users the need to know for

⁸ 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.

accessing a document.

2. These markings cover some of eu-LISA's core administrative activities and may only be used in accordance with the given restrictions.
3. 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.
4. 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 eu-LISA to personnel with a need to-know.
5. These markings cover some of eu-LISA's core administrative activities and may only be used in accordance with the given restrictions.
6. 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.
7. 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 Departments or services; or
 - An agreed workgroup name or other designation.
8. Annex 1 identifies all of the markings from the former Security Notice 01 (eu-LISA No/19-2015) on the use and application of markings, and their equivalents under the current scheme.
9. The Security Unit shall prepare and maintain the list of distribution markings, including where appropriate, a list of reserved distribution markings with details on their use.

Abbreviated names

10. 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:
 - Operations Department , e.g. 'Ops Dpt';
 - Corporate Service Department, e.g. 'CSD';
 - Corporate Service Department – Human Resources Unit, e.g. 'CSD.HRU'.

Multiple entities may be specified, separated by commas. eu-LISA departments must

always be specified using their standard abbreviations (e.g. CSD, OPS, SEC).

Working groups or other designations

11. 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 Departments or from outside eu-LISA. 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.
12. Consequently, group names must be formally defined and agreed between the leading responsible of a working group, the eu-LISA Security Unit and the Document Management Officer (DMO). The eu-LISA Security Officer must keep a record of all group names. When this option is used, the document may be shared within the defined audience. While some flexibility in sharing such documents within eu-LISA may be allowed where there is a business need, they must not be shared with third parties without authorisation from the originator⁹.

Other distribution markings

13. 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.

a. 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)*.

b. 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:

⁹ The originator in this case refers to the service that bears the legal responsibility for protecting the document or information within eu-LISA.

RELEASABLE TO: EUROPEAN PARLIAMENT

The reliability marking shall offer clear understanding of which groups or persons within the named organisation or third party are authorised to receive the document.

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.

c. TLP markings

The Traffic Light Protocol¹⁰ markings *TLP AMBER* and *TLP RED* may be used in combination with the eu-LISA 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 eu-LISA. They must not be implemented in corporate CISs.

Examples:

SENSITIVE: TLP: AMBER

Chapter 2 APPLICATION OF MARKING

Article 6 Markings in documents

1. The main security marking (SENSITIVE) must be in Corbel, font size 11, bold, and in capital letters¹¹. Distribution markings must follow a colon and be in Corbel 11, italics, as given in this document, e.g. '*Management*'.
2. 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. 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.
3. 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). 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

¹⁰ See <https://www.first.org/tlp/> for the definitions of the levels and further information.

¹¹ Following the Agency Visual Identity Manual.

normal text at the standard font size of the header in the centre of the header.

4. 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).

Article 7 Markings in communication and information systems (CISs)

Email

1. 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 the security markings and other instructions. In line with the established practices across eu-LISA, secure emails should be handled as **SENSITIVE**, even when not marked.

Web-based CISs

2. 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.

Document handling systems

3. Document handling systems must clearly indicate any security markings applied to the document before it is opened, as well as in the document itself. Further information on the implementation of security markings in individual systems must be provided by the system owner.
4. 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.

Other CISs

5. 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.
6. 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, if available, may also be included.

7. 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.
8. All printouts containing SNC information must bear the appropriate markings.

Article 8 Markings in document metadata

1. Where a system records metadata about the document (title, author, creation, date, etc.) this must also include the security marking to enable the system to display the markings to users and to transfer documents to other systems and ensure consistent handling.
2. Each document should include a property named 'Security marking' which will contain the marking "SENSITIVE". Other properties may be included for the distribution markings.

Chapter 3 HANDLING INSTRUCTION FOR SNC INFORMATION

Article 9 Handling instructions for SNC information marked SENSITIVE

1. The standard handling instructions apply to all documents bearing the marking **SENSITIVE**.
2. Where necessary, mandated personnel¹² may specify additional handling instructions.

Creation

3. Creation comprises 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.

4. Each document containing SNC information must include either:

¹² Under Article 10 of Management Board Decision 2016/133 REV3 or Regulation (EU, Euratom) 2016/2030 amending Regulation (EU, Euratom) No 883/2013, as regards the secretariat of the Supervisory Committee of the European Anti-Fraud Office (OLAF), (OJ L 317, 23.11.2016, p. 1).

- a footnote with a link to the standard handling instructions (optionally including a summary of the main handling instructions), or
 - the handling instructions themselves.
5. Where applicable during the creation of SNC information, the author of a document may select the appropriate distribution marking, based on the subject matter and the level of damage that may be caused by unauthorised disclosure.

Handling

6. Handling includes the instructions for reading, editing, copying, scanning, printing and storing documents.
7. Recipients shall distribute SNC information on a need-to-know basis, bearing in mind the principle of professional secrecy and the obligations under the Staff Regulations (Article 17)¹³.
8. When handling SNC information, recipients shall take the necessary measures to ensure that the information is not released outside the EU institutions, agencies and bodies and Member States' public administrations without permission from the originator.
9. Documents shall not be left 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.
10. Electronic copies should be stored on platforms that can only be accessed by the target audience. Where appropriate, the use of encryption and digital signatures shall be used, taking into account the risks and other countermeasures in place.
11. Scanned copies of documents, including both electronic and hard copies, shall 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.
12. Documents should be removed from printers, photocopiers, faxes or other shared devices immediately.

¹³ Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (Conditions of Employment of Other Servants) (OJ L 56, 4.3.1968, p. 1).

Distribution

13. Distribution comprises 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.
14. Distribution is on a need-to-know basis, and the information is not to be distributed outside of the audience indicated.
15. When distributing SNC information, the handler shall make sure that the recipient is aware of the applicable handling instructions.
16. Any person receiving SNC information who is not the intended recipient shall inform the sender, where possible, and destroy the information by appropriate secure procedures.
17. Where physical mail is used for distribution, the information shall be closed¹⁴ inside an opaque envelope.
18. Where email is used to transmit SNC information, even partially, outside the Agency, the use of digital signatures and/or encryption is mandatory to assure data integrity and confidentiality.

Downgrading and destruction

19. 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.
20. 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)¹⁵. Shredded documents may be disposed of in normal office waste.
21. Documents stored on electronic media must be purged¹⁶. If the media is not to be

¹⁴ 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.

¹⁵ This instruction is without prejudice to the provisions of Commission Decision 2002/47/EC, ECSC, Euratom of 23 January 2002 amending its Rules of Procedure concerning provisions on document management (OJ L 21, 24.1.2002, p.23) and Commission Decision 2004/563/EC, Euratom amending its Rules of Procedure concerning Commission's provisions on electronic and digitised documents (OJ L 251, 27.7.2004, p.10).

¹⁶ The method of purging depends on the type of medium as follows:
Magnetic tapes — degaussing;
Magnetic disks — degaussing or overwriting with approved software;

reused, they must be returned to the Security Unit who will proceed with their physical destruction.

Chapter 4 OTHER ISSUES

Article 10 Personal information

1. 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 and in some cases Security matter).
2. Personal information must be handled in line with Regulation (EU) 2018/1725. The Data Protection Officer shall 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 eu-LISA 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 eu-LISA documents containing personal data.

Article 11 Archiving and access to documents

1. 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 information¹⁷.
2. The rules for the handling of marked documents are to be applied without prejudice to Regulation (EC) No 1049/2001 and Decision No 2016-026 laying down practical arrangements regarding public access to the documents of the Agency¹⁸. Any document held by eu-LISA, including documents containing sensitive information,

Flash memory (USB keys, SD cards, SSD drives, etc.) — overwriting with approved software;
Non-rewriteable media (optical disks, non-volatile solid-state devices, smart cards ...) - physical destruction.

¹⁷ For instance giving access to involved stakeholders as per hierarchy's request.

¹⁸ Decision No 2016-026 of the Management Board of the European Agency for the operational management of large scale IT systems in the area of freedom, security and justice of 28 June 2012 laying down practical arrangements regarding public access to the documents of the Agency for the operational management of large scale IT systems in the area of freedom, security and justice.

may be subject to a request for public access to documents and must be assessed pursuant to Regulation (EC) No 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 (EC) No 1049/2001 in eu-LISA also need to be able to access eu-LISA's documents forming the subject of applications for public access.

Article 12 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;
- Marked documents and translations must be securely deleted from non eu-LISA systems when the translation has been completed.
- Systems used by translators must be configured to ensure alignment with the instructions in Article 10 above.

Article 13 Use of markings with external partners

1. Should eu-LISA need to exchange information with one or more third parties outside eu-LISA, a memorandum of understanding, contract or security convention shall be drawn up between eu-LISA and the external party, setting out the handling instructions for all information exchanged between them.
2. The appropriate handling instructions must be included with any document bearing a marking that is shared with third parties.

Article 14 Exceptions for mandated staff

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

Article 15 Entry into force

1. The present Decision shall enter into force 30 days following its adoption by the Management Board.
2. 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.

Annex 1: CONVERSION TABLE

The table below shows the equivalent new marking for all of the markings from the previous version of provisions for handling SNC information in eu-LISA.

Previous marking	New marking
LIMITED BASIC	No SNC level
LIMITED HIGH	SENSITIVE
LIMITED HIGH [Unit/Group]	SENSITIVE: [Unit/Group]
Embargo	See article 5.13
Releasable to	See article 5.13
Staff matter	SENSITIVE: Staff matter
Security matter	SENSITIVE: Security matter

Annex 2: RESERVED DISTRIBUTION MARKINGS

Distribution markings	Restrictions
Staff matter	To be used only for documents related to active or former staff matters and managed by HR and management concerned, and to be opened by the addressee(s)
Security matter	To be initiated only by the Security function of eu-LISA