ECA Information Classification Policy

Purpose

01 The purpose of this policy is to establish a framework of rules for the European Court of Auditors (ECA) to assess, classify, secure and handle its own and third party information, based on the sensitivity and confidentiality of the information. It aims to ensure that information is properly categorised and handled, and reduce the risk of information leaks, unauthorised modifications or loss.

02 This policy governs the classification and management of "non-EU classified" information throughout the ECA, with a view to applying and maintaining the appropriate level of confidentiality throughout the information lifecycle – from creation or receipt to registration, sharing and exchange, storage, archiving and ultimately destruction. It also refers to "EU classified" information and its four confidentiality categories.

03 This policy complements the ECA's Information Security Policy[1]. It cancels and replaces the previous information classification policy[2]. The application of this policy is supported by general information classification guidelines as well as by guidelines covering specific ECA activities[3].

Scope

04 This policy applies to all information created, held and managed by the ECA, including paper documents and digital information stored on any type of media. It defines the roles and responsibilities of all those involved in managing the information classification – ECA Members, ECA staff members or ECA externals.

05 This policy is without prejudice to:

a) Regulation (EU) 2018/1725[4] 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.

[1] https://intranet.eca.eu/documentcenter/DEC/DEC%20127%2015/DFS066064EN02-15MD-DEC127-15-information_security_policy-ORAN_s2.pdf

[2] https://ecanet.eca.eu/en/secgen/sg3/ECADocuments/DFS070432EN01-15PP-CP-68-ORs.pdf

[3] Guidelines are currently under preparation.

[4] https://eur-lex.europa.eu/eli/reg/2018/1725/oj

b) ECA Decision No 12/2005[5] regarding public access to Court documents as amended by ECA Decision No 14/2009[6].

c) ECA Decision No 6-2019[7] on the open data policy and the reuse of documents.

d) Council Regulation (EEC, Euratom) No 354/83[8] of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community as amended by Council Regulation (EC, Euratom) No 1700/2003[9] of 22 September 2003 and by Council Regulation (EU) 2015/496[10] of 17 March 2015.

Definitions

06 For the purposes of this policy:

a) 'Automated processes' refers to the use of digital technology to perform processes in order to accomplish a workflow or function;

b) 'Availability' means the property of being accessible and usable upon request by an authorised entity;

c) ´CEOS' refers to the Conditions of Employment of Other Servants of the European Union, as laid down by Regulation No 31 (EEC)[11] as amended;

d) 'Classification' refers to the attribution of a confidentiality level to information based on the confidentiality of its content;

e) 'Document' means any recorded information, regardless of its physical form or characteristics;

f) 'ECA externals' comprises trainees, service providers working on the ECA's premises (intra-muros) and/or on their own premises (extra-muros);

g) 'ECA staff' comprises officials, temporary staff, contract staff and seconded national experts;

---

5 https://intranet.eca.eu/documentcenter/Decisions/Decision%20012%2005/012en_EN.pdf

6 https://documentcenter.eca.eu/officialdocuments/Decisions/Decision%20014%2009/014en_EN.pdf

7 https://documentcenter.eca.eu/officialdocuments/Decisions/Decision%20006%2019/SGL108714EN02-19MD-D-006-2019-ORs.pdf

8 http://data.europa.eu/eli/reg/1983/354/oj

9 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003R1700

10 https://eur-lex.europa.eu/eli/reg/2015/496/oj

11 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01962R0031-20200101

h) ‘European Union classified information’ (EUCI) means any information or material to which an EU security classification is applied;

i) ‘Information’ means any written or oral information, whatever the medium and whoever the author. Information can both be created by the ECA and / or received from third parties;

j) ‘Information breach’ means any action or omission causing partial or complete disclosure of non-public information to unauthorised persons or loss of such information;

k) ‘Information originators’ refers to third parties which provided information to the ECA. For audit information, the body or individual from whom the information is obtained is considered the originator of the information;

l) ‘Information System’ refers to a system that stores and manages information in digital form;

m) ‘Integrity’ means the property of safeguarding the accuracy and completeness of assets and information;

n) ‘Non-EU classified information’ (non-EUCI) means information not classified as EUCI. The ECA classifies this information as either ‘Sensitive’, ‘ECA use’ or ‘Public’ (‘ECA confidentiality level’);

o) ‘Premises’ mean any immovable or assimilated property and possessions of the ECA;

p) ‘Service Level Agreement’ (SLA) is a contractual commitment between the ECA and a service provider, which specifies particular aspects of the service including provisions regarding the security of information they receive from, or in respect of, the ECA;

q) ‘Staff Regulations’ means the Staff Regulations of Officials of the European Union as laid down by Regulation No 31 (EEC) as amended;

r) ‘Third party’ means any natural or legal person, or any entity outside the Court of Auditors, including the Member States, other EU or non-EU institutions and bodies, and third countries.

Principles

07 Security of information requires taking all reasonable measures to protect information from unauthorised access, use, disclosure, modification or destruction.

08 The following principles govern this policy and any related guidelines developed in the future:

I. Professional discretion

09 The rules and guidelines laid down in this policy are based on the ECA staff's obligation to refrain from unauthorised disclosure of information received in the line of duty, as provided for in Article 17 of the Staff Regulations[12] and the relevant ECA ethical framework[13].

II. Need-to-know

10 The exchange of non-public information between ECA Members, ECA staff and ECA externals should be limited to only such information as they need to obtain to carry out their duties. ECA Information System users and automated processes must only be given the access rights they require in order to perform their tasks.

Policy

11 Non-EU classified information is assessed based on the harm its unauthorised disclosure and/or alteration may have on the interests of the ECA, its Members and staff, EU Institutions or bodies, or any other third party. The result of this assessment determines the ECA confidentiality level.

12 When aggregated information contains elements bearing different confidentiality levels, the highest of those levels must apply.

13 Information received from other EU Institutions or third parties must retain the level of confidentiality assigned by the originating party, and be allocated an ECA confidentiality level at least as high.

14 The information processed by our institution will always be kept and processed with the utmost care to preserve its integrity and the appropriate level of availability.

[12] For temporary and contract staff this article is applicable by analogy through Articles 11(1) and 81 CEOS.

[13] https://www.eca.europa.eu/en/Pages/Ethics.aspx

15 If a Memorandum of Understanding (MoU) referring to data exchange is signed with other official bodies, it must contain a correlation table between their classification levels and ECA classification levels.

16 Based on these principles, all information created, collected or received by the ECA is assigned one of the following confidentiality levels (ECA USE is the confidentiality level by default, except for EUCI or for information specifically assigned with another confidentiality level) :

I. PUBLIC

Information created, collected or received by the ECA that, due to its content, can be made accessible to the outside world, without harm. This includes information collected or received from public sources, as well as the information resulting from its professional and administrative activities that the ECA decides to make public, notably in the form of published documents.

II. ECA USE (default)

Working level non-public information created, collected or received by the ECA in the course of its professional and administrative activities, and to which the general principle of professional discretion, provided for in Article 17 of the EU Staff Regulations[14] and the relevant ECA ethical framework, applies and which does not fall into higher categories.

The access to ECA USE information is granted on a need-to-know basis to ECA staff and ECA externals - according to the different stages of the audit process, or other information processing activities to which they are assigned.

III. SENSITIVE

Information which the ECA must protect because of legal obligations laid down in the Treaties, or other legal acts, protecting the rights and interests of the EU Institutions, individuals or legal entities.

The ECA has the obligation to ensure strict non-divulgence of SENSITIVE information to non-authorised people through specific handling and storage procedures.

[14] For temporary and contract staff this article is applicable by analogy through Articles 11(1) and 81 CEOS.

Access to SENSITIVE information is subject to the explicit approval of the information owner.

IV. EU CLASSIFIED

'EU classified information' (EUCI) is any information to which an EU institution or Member State has assigned one of the following levels:

RESTREINT UE / EU RESTRICTED: information and 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 European Union or of one or more of the Member States;

CONFIDENTIEL UE / EU CONFIDENTIAL: information and 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 European Union or of one or more of the Member States;

SECRET UE / EU SECRET: information and 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 European Union or of one or more of the Member States;

TRÈS SECRET UE/EU TOP SECRET: information and 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 European Union or of one or more of the Member States.

Roles and responsibilities

17 An **information owner** is the President, a Member, the Secretary-General, a director, a chairperson of any of the ECA committees or any other ECA staff member with responsibility for a procedure through, or for which, information is created, collected and/or received. The information owner is responsible for ensuring that information which falls under her / his responsibility is classified and managed in accordance with this policy and its guidelines.

18 As regards the information associated with an audit task, the information owner is the reporting Member. The information owner can designate and delegate her / his tasks to an information manager (i.e. a director, a principal manager or a head of task).

19 The **information manager** is responsible for supervising and reporting on the handling, management and protection of the information on behalf of the information owner.

20 **Information user** — any ECA Member, ECA staff member or ECA external that interacts with information.

a) All ECA staff are bound by the confidentiality obligation and undertake to respect the duties of confidentiality and non-disclosure based on Article 17 of the Staff Regulations[15].

b) All ECA externals are required to comply with confidentiality and non-disclosure rules within their contractual obligations with the ECA.

c) All ECA staff and externals are responsible for handling information in accordance with the ECA classification level set by the information owner.

d) All ECA staff and externals must report issues in relation to the application of this policy to the information manager.

21 **Information custodians** — for information stored in information systems: ECA IT service managers responsible for implementing, maintaining and backing up the systems, databases and servers that store ECA information.

22 **Information custodians by contract** — external entities or companies contracted for implementing, maintaining and backing up the systems, databases and servers that store the ECA's information. Applicable security measures are defined in an SLA between the ECA and the contractors.

23 **Information Security Officer** is responsible for the security of all information.

24 **Data Protection Officer (DPO)** is responsible for the protection of personal data owned and/or processed by the ECA.

25 **Head of Security** is responsible for implementing the physical security measures and procedures necessary to protect the information.

26 The ECA Information Classification Guidelines and specific guidelines further specify the roles and responsibilities of the above-mentioned actors, with the objective of ensuring and facilitating the practical implementation of this policy.

[15] For temporary and contract staff this article is applicable by analogy through Articles 11(1) and 81 CEOS.

Handling of information breaches

27 Any ECA member of staff or ECA external becoming aware of a breach or suspected breach of security must report it immediately to the Information Security Officer.

28 Any individual who is responsible for compromising or losing EU classified or sensitive information may be liable to disciplinary action in accordance with the Staff Regulations. That disciplinary action shall be without prejudice to any further legal or criminal proceedings by the competent national authorities of the Member States in accordance with their laws and regulations[16].

29 All appropriate measures must be taken to:

a) inform the originator of the information (when received from a third party);
b) ensure that the case is investigated by personnel not immediately involved in the breach in order to establish the facts;
c) assess the potential damage caused; and
d) take appropriate measures to prevent a recurrence.

30 If any defects or breaches are identified in the protection of information in an IT system, these must be reported to the Information Security Officer.

31 If any defects or breaches are identified in the protection of physically stored information, these must be reported to the Head of Security.

32 If any personal data is concerned, the DPO must be informed.

33 Where EU classified information is also concerned, the procedure concerning the security rules for protecting EU classified information[17] needs to be followed.

[16] See Article 86 and following of the Staff Regulations and Articles 6 and 7(1) of the Code of conduct for the Members of the Court.

[17] ECA Decision 16-2020 on the security rules for protecting EU classified information under preparation.