14 December 2016
EMA/174602/2016
Executive Director

Document classification policy

POLICY/0081

Status: PUBLIC
Effective date: 13/12/2016
Review date: 13/12/2019
Supersedes: n/a

Table of contents

1. Introduction and purpose 2
2. Scope 2
3. Definitions 2
4. Policy Statement 3
5. Roles and Responsibilities 3
5.1. RACI 4
6. Criteria for documents classification 5
6.1. Classification scheme 5
7. Related documents 6
8. Changes since last revision 6
9. Annexes 6

30 Churchill Place ● Canary Wharf ● London E14 5EU ● United Kingdom
Telephone +44 (0)20 3660 6000 **Facsimile** +44 (0)20 3660 5555
Send a question via our website www.ema.europa.eu/contact

1. Introduction and purpose

Documents are a critical asset at the Agency and the appropriate and timely sharing allows internal and external stakeholders to move synergistically towards common objectives to enforce Agency's trust and transparency.

This policy defines the classification scheme which supports the Agency in identifying documents criticality level and the appropriate security measures to be applied.

2. Scope

This policy applies to all documents held at the Agency.

3. Definitions

Information	Information[1] is any aggregation of data, which has a value and a meaning for the Agency.
Data[2]	**Structured**: Content tagged for machines to read and parse. Typical structured data is referred and stored in databases.
	Unstructured: Text heavy content on which nothing can be readily classified or stored in a structured format. Unstructured content is designed for humans to read and extract key information. Some examples are Spreadsheets, emails, correspondence etc.
	Semi Structured: is still text heavy but also has content that can be parsed out and categorised. Documents with associated metadata or information tagged on a website to make it searchable by a computer are example of semi structured content.
Document	"document[3]" shall mean any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) held by the Agency.
EMA Staff	Temporary Agents (TA), Contract Agents (CA).
Internal Users	Group **A**: EMA Staff.
	Group **B**: Seconded National Experts (SNE), Interims and Trainees.
	Group **C**: Contractors (onsite/offsite).
Committee, Working Parties and Management Board Members[4]	Members of EMA scientific committees to carry out scientific assessments. Members of EMA working parties. Management Board members not included in EMA Staff population.
Network	**European** – European Medicines Agency, the EU national medicine competent authorities with responsibility for regulation of human and/or veterinary medicinal products, the European Commission.
	International – Internationals organisations with appropriate confidentiality agreements in place with the EMA.
Applicant	Procedure Applicant (e.g. Marketing Authorisation Applicant and Marketing Authorisation Holder).

[1] Therefore, the concept of information is very wide and various; for example, any news, written or oral communication, data in a file or the code in a program can be considered as information, information can be received, processed or published.
[2] Source: AIIM Association for Information and Image Management
[3] Definition provided in the Regulation (EC) No 1049/2001 - European Parliament
[4] Including alternates but not observers

4. Policy Statement

The main objective is to protect the Agency's reputation preventing risks of document's unauthorised access or misuse[5] through classification and handling. The overarching principle of this policy is that if a document potentially contains elements that require specific protection, even if these elements are minimal, such document should be classified appropriately in order to protect those elements.

The Agency will achieve this by:

1. Defining the Agency's documents classification schema and guidelines;
2. Assigning responsibility to the existing process owners to act as document classification owners for defining the correct document classification for documents managed in their process(es) and supervise the implementation of the relevant protections;
3. Evaluating the documents classification changes during their lifecycle and in line with the evolution of information relevance; documents classification may change due to the document lifecycle or due to specific legal requirements.
4. Compliance, as a minimum, with all applicable legislation and Agency requirements;

The Agency will enforce this by:

5. Provision of adequate and appropriate resources to implement this policy and to ensure it is adequately communicated and understood;
6. Effective communication and cooperation with stakeholders/user to raise awareness.

5. Roles and Responsibilities

Documents classification and handling is everyone's responsibility and a prime responsibility of all levels of management. It is expected everyone to contribute towards achieving the Agency's overall security, trust and transparency objectives.

Head of Division, Head of Department and Head of Service

Will be consulted on all matters relating to policies and procedures and are responsible for promoting adoption within their respective areas of operation.

Ensuring all staff is aware of their responsibilities in terms of documents classification and receives appropriate guidance and training relevant to their job role.

Ensuring appropriate notification of any violations of this policy, especially those resulting in breaches that are subject to data protection law or other applicable law.

Process Owners[6] as Document Classification Owner

Must understand the nature of the documents managed within their process(es) and are therefore responsible for specifying, implementing and monitoring safeguards to protect the confidentiality, integrity and availability of these documents throughout their lifecycle. This includes establishing effective controls which manage the creation, storage, access, distribution, amendment, copying, archiving and disposal of documents.

[5] Including modification, removal or destruction during storage, transport, re-assignment, and disposal
[6] Process owner role and responsibilities are defined here: EMA/576906/2014 , 3.2 Process Owner responsibilities EMA , https://docs.eudra.org/webtop/drl/objectId/090142b2832553e9 The list of process owners is available here: EMA/291743/2015 , 3.4 Process Owners https://docs.eudra.org/webtop/drl/objectId/090142b28329f9d0

Perform an evaluation of the documents managed within the process for which they are responsible in order to define the appropriate classification level.

Periodically review and assess document classifications, and adjust them as required.

Information Security Service

Shall establish and monitor the implementation of the documents classification policy approved by the Executive Director.

Shall enforce the system security to meet the policy compliance.

Support the process owners and Users providing guidelines.

Information Management

Shall update and maintain this policy as the policy owner

Shall oversee and coordinate the implementation of the classification in order to assure consistency across the Agency.

Users

Unless automated marking is provided, mark the document (created or received) in accordance with process owner evaluation.

All authorised Users who have access to documents are required to keep them secure to the level required by the process owner.

In accordance with the document lifecycle, user updates the document marking, unless automated marking is provided.

Must ensure compliance with this policy and be responsible for his/her activities.

Must report any violations of this policy to the Information Management Security Team and IT Service Desk.

5.1. RACI

R = Responsible, A = Accountable, C= Consulted, I = Informed

Responsibilities	***Head of Division, Head of Department, Head of Service***	***Document creator, approver, recipient***	***Process Owner*** *as Document Classification owner*	***Information Management***	***Information Security***	***Internal Audit***
1. Promote adoption of the policy and ensure all staffs are aware of their responsibilities	***Responsible Accountable***		***Consulted***	***Consulted***	***Consulted***	
2. Oversee classification process: • Assure consistency across the Agency	***Consulted***		***Informed***	***Responsible Accountable***	***Consulted***	***Informed***
3. Support the Process Owners/Users: • provide guidelines • enforce system security			***Consulted***	***Consulted***	***Responsible Accountable***	***Consulted***
4. For his own documents evaluate the data classification lifecycle and oversee the classification and handling process			***Responsible Accountable***	***Consulted***	***Consulted***	***Informed***
5. Unless automated, mark information in accordance with classification lifecycle defined by the process owner and, if needed, mark the need to know specifying the restricted population		***Responsible***	***Accountable***	***Informed***	***Consulted***	***Informed***
6. Manage information in accordance to the guidelines		***Responsible***	***Accountable***			
7. Periodically evaluate changes to the defined data classification lifecycle			***Responsible Accountable***	***Informed***	***Consulted***	***Informed***
8. In case changes are detected inform and oversee the reclassification process			***Responsible Accountable***	***Informed***	***Consulted***	***Informed***

6. Criteria for documents classification

Documents are classified considering, at least, the following aspects:

1. All EMA documents must be classified as **Public, Internal, Confidential** or **Restricted**. Each classification can be accessed by a specific **predefined population** considering:
   - The sensitivity of the document **inside and outside the Agency** and the risks associated with the document;
   - The **negative impact** of document unauthorised access, loss and/or destruction.

2. If needed, **"Need to know"** must be explicitly marked, and the restriction of who can access the document must be defined[7].

3. All the documents must be marked by the document creator/recipient/approver in accordance to the evaluation defined by the process owner, and treated with the required security measures.

4. EMA classification must also comply with Data Protection Law (in particular Regulation (EC) No 45/2001) and is without prejudice to Regulation (EC) no 1049/2001 on Public Access to documents.

5. If elements of different nature are present in a document, the classification applied to this document will be the **more restrictive**. Therefore, if the document contains elements that require specific protection, even if these elements are minimal, such document should be classified appropriately in order to protect these elements.

6.1. Classification scheme

Public - Documents already exposed to the public or authorised to be exposed to the public.

- Predefined Population: Everyone (e.g. General Public).

Internal - Documents not available to the public, the unauthorised disclosure of which could be **disadvantageous to the interests of the Agency**.

- Predefined Population[7]*:* All internal Users, Internal documents disclosure outside the Agency is driven by the "need to know" criteria (these documents are available only to authorised person to perform their job/activity) and under proper non-disclosure and restricted use obligations[8].

Confidential - Documents not available to the public. Unauthorised disclosure could **seriously harm the interests of the Agency and/or its network**; if disclosed, both internally and externally, can cause serious damage to the Agency's reputation and/or its network reputation. These could be characterised by the fact that they may at some stage be made available to the public, but that their premature disclosure might be prejudicial.

- Predefined Population[7]*:* These documents are disclosed by default to all **Internal Users of group A** (EMA Staff). It is also disclosed on a need-to-know basis to **Internal Users of group B** (Interims, Trainees and Seconded National Experts), to Committee Members, to the **Network** to the **Applicant.**

[7] Excluding personal data, the access to which will be based on need to know basis and managed in accordance with Data Protection law requirements

- Restrictions: All documents designated as Confidential are prohibited from disclosure outside the EMA except with the approval of the Document Classification Owner and under strict obligations of non-disclosure and restrictions on use with no fixed term or end to such obligations[8].

Restricted - Documents not available to the public and with limited internal access. Unauthorised disclosure could **extremely harm the interests of the Agency and/or its network**; if disclosed, both internally (i.e. to persons outside the specific subset of EMA staff mentioned below) and externally, could cause serious damage to the Agency's reputation and/or its network reputation.

- Predefined Population[7]*:* These documents are made available only to the Executive Director[7] and possibly to other EMA staff on a strict need-to-know basis.
- Restrictions: All documents designated as Restricted are prohibited from disclosure outside EMA except with the approval of the Document Classification Owner and under strict obligations of non-disclosure and restrictions on use with no fixed term or end to such obligations[8].

7. Related documents

- Internal guidance on document classification and handling.

This document contributes to the achievement of the following ISO 27001:2013 requirement:

- A.8.2.1 Classification information
- A.8.2.2 Labelling of information
- A.8.2.3 Handling of assets
- A.13.2.2 Agreements on information transfer

8. Changes since last revision

n/a

9. Annexes

n/a

London,

[Signature on file]

Guido Rasi

Executive Director

[8] Non-disclosure agreements are already in place with specific third parties of EMA network (e.g. competent authorities of the EU Member States).