esma European Securities and Markets Authority

Information and Records Management

Procedure

ESMA61-23-513

Table of Contents

1 Document information and approval

Document information			
Version:	1.0	Document number:	ESMA61-23-513
Status:	Adopted	Effective date:	18/04/2017
Classification:	ESMA Regular Use	Review date:	17/04/2020
Supersedes:			

2 Introduction

Within the framework of ESMA's Information and Records Management policy, the purpose of this procedure is to define the process of creation and management of records in ESMA's processes and systems. The Annex 1 in a separate document (Filing and retention referential – ESMA61-23-528) applies to documents, mails and databases.

As stated in the policy (ESMA61-23-461), ESMA is committed to establishing and maintaining records management practices that meet the regulations and requirements that ESMA has to comply with, ESMA's business needs, accountability requirements, professional secrecy, safety, continuity and stakeholders' expectations.

The intended audience of this document is ESMA staff and contractors.

3 Purpose and scope

This procedure applies to ESMA staff and contractors, to all aspects of ESMA's business and all information created, received and managed by ESMA in-house and off-site.

4 Legal basis

ESMA has to comply with general EU legal and regulatory requirements for documents, records and archives management. These legal requirements are defined in ESMA's policy (ESMA61-23-461).

5 Reference documents

This procedure is aligned with the following policies and procedures:

- Decision on Access to documents (ESMA/2011/MB/69).
- Decision on Data Protection implementing rules (ESMA/2011/MB/57).
- Information Security policy (ESMA/2014/INT/130).
- Data Classification policy (ESMA/2014/INT/134).
- Data Retention and Disposition policy (ESMA/2014/INT/136).

Other reference documents are listed in the Policy (section 6 – Reference documents and section 18 – Annex 3).

Additional information on the implementation of this procedure can be found in:

- Annex 1: Filing and retention referential (ESMA61-23-528)

- Work instructions - See: https://wiki.esma.europa.eu/display/ODM/Document+Management+Work+Instructions

6 Definitions

Access: The ability to use, modify or manipulate an information resource.

Archives: Permanent records, maintained for continued use (ISO 15489-1).

Authenticity: The persistent context of a record related to the action that it tracks, the identity of the actor and the time and date.

Availability: The protection of IT systems, and data, to ensure that access and use of information by authorised users is timely and reliable.

Confidentiality: Protection of sensitive information, which prevents disclosure to unauthorised individuals, entities or processes.

Data: A discrete fact or characteristic.

DIFEA: Data Integration For ESMA Analytics – the ESMA data analysis tool allowing ESMA users to analyse and manipulate all data in its databases.

EDRMS: **Electronic Document and Records Management System**: An information system that captures, manages and provides access to records over time (ISO 15489-1).

Information: Data combined in context.

Information asset: An information set that is defined and managed as a single unit so that it may be understood, shared, protected and exploited effectively.

Integrity: A record that has integrity is one that is complete and unaltered (ISO 15489-1).

IRM: Information and Records Management.

Metadata: Metadata for records should support usability by providing information needed to authenticate, retrieve and present them.

Record: Information created, received and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business (ISO 15489-1).

Records Management: Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions (ISO 15489).

Reliability: The attribute of a record that captures a full and accurate representation of the transactions, activities or facts that it tracks. To be reliable a record shall be created at the time of the event to which it relates, or soon afterwards, by individuals who have direct knowledge of the facts, or by systems routinely used to conduct the transaction.

Retention and Disposition policy: Policy that controls how long records are kept and whether at the end of this period, the record is permanently archived or destroyed. *Note: the policy is set by an aggregation of procedures resulting from the analysis of requirements and needs of each business process.*

SHERPA: ESMA's Document Management System (based on MS SharePoint).

Usability: Usable records are those which are easily located, retrieved, presented and interpreted for as long as needed (in accordance with the retention and disposition schedules) and connected to the business processes or the transaction that produced them.

7 What ESMA's records are

ESMA's records are documents, mails, emails, data and information received or created by ESMA's staff in the context of their activities i.e. concerning a matter relating to the policies, activities and decisions falling within the Authority's competence and in the framework of its official tasks.

They can be in any medium: paper, electronic (electronic born or digitised, including emails) or audio visual (voice mail, sound recording, video, photo, film, etc.).

ESMA's information and records shall possess the following characteristics and attributes: authenticity, reliability, integrity, usability and appropriate metadata.

ESMA aims to manage records properly, to meet the regulations and requirements that it has to comply with, its needs, accountability requirements, professional secrecy, safety, continuity and stakeholders' expectations.

Failure to properly create, describe, capture, manage, access and store information could expose the organisation to increased risk and/or inhibit ESMA's ability to carry out its mission. These risks may include:

- reputational damage through negative media coverage; or
- audit findings that highlight poor information governance practice or non-compliance with legislative and regulatory obligations; or
- complaints from stakeholders or the public.

The benefits of compliance with this procedure will be trusted records that have probative value, are well described and can be easily retrieved, are stored in known and secure systems/locations, accessible when needed, and protected from misuse or inappropriate deletion.

8 Records controls

8.1 ABM based filing, classification, data protection and retention rules

ESMA will develop a filing, classification, data privacy and retention database based on the ABM (Activity-Based Management) process analysis as well as on legal, business and security requirements. A version of the filing and retention schedule is annexed to this procedure (see Annex 1).

The filing plan drawn up at ESMA's level consists of a number of headings (ABM activities) which are organised in a hierarchical manner and which reflect all the activities of the Authority, from more general (first level) to most detailed (sub-activity/document type).

8.2 Metadata

ESMA has developed a set of metadata to manage records characteristics in systems. The metadata applicable to documents management is defined in the Document Management work instructions.

8.3 "Evidence capture" features

Features will be added to ESMA's systems to keep the evidence value of records in the coming years.

Regarding the document management system, it means that an audit trail will be kept of the name and function of the authors, the date and time of creation or change. The deletion will be in application of retention rules.

9 Records Management Systems at ESMA

The Electronic Documents and Records Management System at ESMA is built on several components:

- The Document Management System (SHERPA); Outlook Exchange and postal mail process[1]

- The IT systems managed by ESMA.

In addition, several systems have been set up by ESMA to allow exchange of documents.

[1] See relevant mail procedure.

9.1 ESMA’s Document Management System, Outlook Exchange and postal mail

All electronic documents that are related to ESMA will be managed in ESMA’s Document Management System (DMS). This is the place to organise, find and maintain ESMA’s information to support its work. The DMS is composed of two environments that manage the documents:

- SHERPA: the ESMA Document Management System, for Public, Regular and Restricted documents and key emails to store; and

- Travail: for encrypted confidential documents.

9.1.1 SHERPA Document Management System

SHERPA is the main ESMA Document Management System. All records (documents and emails) received and produced by ESMA should be stored in SHERPA except documents that require to be encrypted (Confidential documents).

It ensures that the following principles are respected for any record:

- An enhanced efficiency: the storage of documents accessible by all substantially increases efficiency and enables rapid access to information. A proper document handling in connection with common metadata provide the basis for fast document retrieval across the Departments.

  For these reasons, the duplication of document should be avoided as far as possible so that the control of any document remains easy.

- Transparency and accessibility: the objective is to ensure a transparent user experience by enabling self-service access. SHERPA is the common workplace for all staff members and is “open” to all staff members.

  The information is accessible to all, regardless of whether the creator is available or not, or whether the staff needing access is at the office or not.

  Access could, however, be limited when duly justified (Data protection, copyrights, confidential information, etc.)

- Authenticity and security: SHERPA safeguards the authenticity of the stored electronic information as any change is traceable through the history of the document.

- Preservation of the memory of ESMA: well managed documents in an organised structure, with accurate rules, allow to preserve knowledge and history of ESMA.

SHERPA will enable an electronic management of life cycle and retention periods of documents.

9.1.2 Travail

Travail (V: drive) should be used solely to store encrypted documents until SHERPA allows such feature. All confidential encrypted documents should be stored in Travail.

9.1.3 Outlook Exchange

Emails (and attached documents) created or received in Outlook Exchange which have to be managed as records are to be captured in SHERPA when necessary.

9.2 Databases

9.2.1 IT systems

Whenever new databases and automated systems will be designed, records keeping rules will be part of the requirements, to determine what records should be created and captured by the system and tools that need to be accommodated. This will be the responsibility of Business Process Owners and ICT Project Managers to include these in the projects, with the help of the IRM Officer, the Data Protection Officer and Security Officer.

9.2.2 DIFEA Server

Small databases managed by the Departments should be stored on the DIFEA server. The DIFEA server aims at being the central place for small databases (such as large Excel sheet, Access databases or csv files collected by the Departments).

9.3 Communication channels

ESMA has in addition several communication channels to exchange documents with stakeholders. These channels do not constitute the ESMA Document Management System and do not provide the required features in terms of security, retention, archive, collaboration as the Document Management Systems. The main systems in place to exchange documents with stakeholders are:

- The Website – for documents classified as ‘Public’;
- The Extranet – for documents classified as ‘Regular’; and
- The Vault – for documents classified as ‘Restricted’ or ‘Confidential’.

These communication channels should not be considered as places to store documents for ESMA in the long term, but rather allow stakeholders to access a subset of the documents that ESMA produces for certain purposes.

9.4 U: Drive

U: drives are to be used for ESMA staff's personal files only.

9.5 Paper documents

ESMA aims at reducing to the strict minimum the usage of paper documents. All relevant paper documents should be scanned and filed electronically in SHERPA. Produced documents should also be first considered to be created and stored electronically.

The maintenance and storage of the original version of paper documents (after scanning) should be reduced to the following non-exhaustive list:

- Key contracts;
- Financial documents;
- Registration documents of supervised entities, and
- Key supervision documents.

The paper mail procedure as well as the Document Management work instructions provide guidance on the actions applicable to paper documents whenever relevant.

10 Records processes

10.1 Creation and capture

ESMA staff should ensure that they create official records of all decisions and actions made in the course of their official business. For example, if business is transacted by telephone, file notes of the key points in the conversation should be documented. Official meetings should include the taking of minutes.

To assist in promoting the responsible creation of records, the capture of essential information and the management of records over time, ESMA has developed templates and work instructions.

Records are registered in Records Management Systems (such as SHERPA) and given a unique number/identifier. Documents, emails and mails referencing and naming rules are to be found in the Document Management work instructions.

10.2 Access

Accurate search functions, based on ESMA’s activities ontology (see Annex 1) and metadata will be put in place in each ESMA’s records systems, and as much as possible global search will be added.

Records must be available to all authorised staff that require access to them for business purposes.

All access to documents will be tracked in the framework of ESMA’s systems and part of the record life cycle metadata.

All access to ESMA’s records by members of the public, will be managed in accordance with the Access to Information legislation, and ESMA’s access to documents decision (ESMA/2011/MB/69). The filing, classification, data privacy and retention rules database, developed in the framework of the IRM policy and procedure, are soundly based on the analysis of all applicable requirements.

10.3 Retention and disposition

ESMA’s records are managed in accordance with the filing, classification, data privacy and retention rules database (see filing and retention referential, Annex 1).

Administrative records such as financial and personnel records are covered under the EC common retention rules, incorporated in ESMA’s retention rules.

No ESMA’s record can be disposed of unless in accordance with these retention and disposal authorities.

Approval and signed authorisation for retention, destruction or transfer of records must be sought from the appropriate staff (IRM Officer, Business Process Owner, ICT Project Manager) according to the responsibilities assigned below before any disposal takes place.

Track of all disposal actions should be kept. Metadata of records should be kept in Records Management Systems even after records deletion.

10.4 Maintenance and monitoring

The IRM Officer and the SHERPA Project Manager are responsible for ensuring that records and environmental conditions are monitored regularly to protect records.

The IRM Officer is responsible for the physical records storage condition. This includes checking temperature and humidity levels in dedicated records storage areas for paper records.

The Head of the ICT Unit, the ICT architects, the ICT Managers are responsible for ensuring that digital records are backed up, refreshed or replicated when scheduled, when new storage devices and media are being installed or when degradation is detected.

Maintenance of electronic records can also entail the migration of data. Migrations must be authorised by the IRM Officer and must produce authentic, complete, accessible and useable records.

ESMA has implemented a number of security and business continuity measures, including information security policies, as part of its Information Security Management System (ISMS), for safeguarding its information assets. Staff should abide by these measures at all times.

10.5 Transfer

ESMA has an on-site storage facility for the storage of physical records that are infrequently used for business purposes but still need to be retained according to the Retention and Disposal Authority. The IRM Officer is responsible for transferring these records to the facility, with the help of the Facility Management team.

Digital and physical records required for transfer to the European University Institute (EUI) will be first kept in ESMA’s archives facilities or systems (on-site or off-site, in accordance with the records and archives policies and procedures). Then they will be transferred to the archival custody of the EUI.

11 Roles and responsibilities

ESMA Senior Management endorses this procedure, recognises the importance of Information and Records Management within the Authority and requires staff to comply with its requirements.

ESMA Senior Management delegates responsibility of implementing this procedure to the Head of the Resources Department.

The Head of the Resources Department is responsible for the implementation of this procedure, and its convergence with IT, security, data protection and ESMA’s procedures (in collaboration with the Head of the Legal, Convergence and Enforcement Department). He/she ensures that it is adequately resourced.

Under the leadership of the Head of the Resources Department, the Information and Records Management Officer is responsible for developing the IRM procedure in collaboration with managers and officers from Legal, Data Protection, Security and IT areas, and with the SHERPA Project Manager.

12 Awareness campaign

The approved procedure will be published on ESMA's intranet. It will also be promoted via staff meetings and specifically convened awareness raising sessions, if required.

13 Consultation status

Prior to its approval, this procedure has been sent for consultation to all Heads of Departments, the Legal Officer, the Internal Control Officer, the Security and Data Protection Officers, the Head of the ICT Unit.

14 Data protection

Any personal data identified in the information affected by this policy shall be handled in compliance with the requirements laid down in Regulation (EC) No 45/2001 and ESMA's Decision on Data protection implementing rules (ESMA/2011/MB/57).

15 Records

The filing of the original copy and the electronic versions of this document is handled by the Resources Department.

16 Final provisions

This procedure will enter into force on 18 April 2017.

It will be reviewed whenever considered necessary and appropriate, but not later than three years following its adoption.