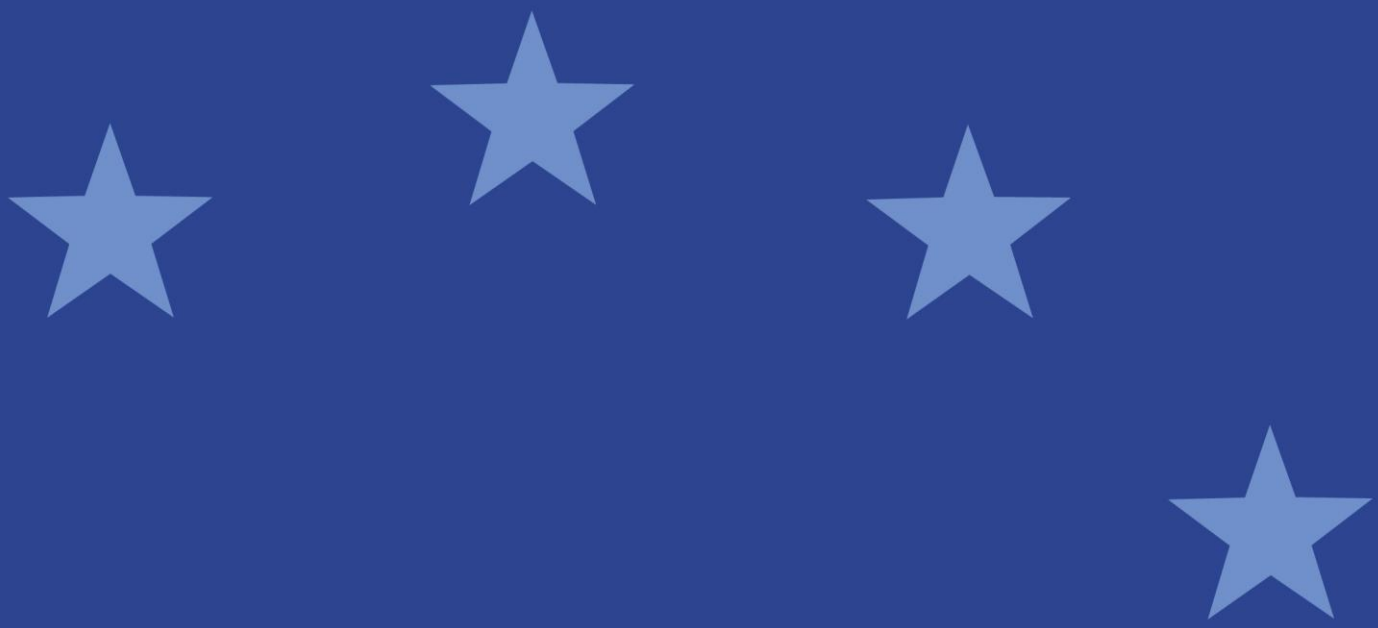
esma European Securities and Markets Authority

Information and Records Management (IRM)

Policy



ESMA61-23-461

Table of Contents

1 Document information and approval

Document information			
Version:	1.0	Document number:	ESMA61-23-461
Status:	Adopted	Effective date:	18/04/2017
Classification:	ESMA Regular Use	Review date:	17/04/2020
Supersedes:	N/A		

2 Definitions and abbreviations

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.

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.

Information governance: Activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs. (Information Governance Initiative, 2014).

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.*

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.

3 Introduction

The necessity for organisational information governance is increasing, as both societal expectations and EU regulation require greater transparency and accountability. ESMA, as the industry monitoring and standardisation regulator for securities and markets, also supports this trend by recommending good practice in data, information and knowledge management and recordkeeping[1] to organisations under its supervision.

This policy, together with the internal policies and strategies on:

- Information Security (ESMA/2014/INT/130),
- decisions on Data Protection implementing rules (ESMA/2011/MB/57) and Decision on Access to Documents (ESMA/2011/MB/69), and
- the Information Technology Strategy "ESMA IT Strategy 2016-2020" (ESMA/2015/ITMG/84).

aim to build an information governance framework. This framework will play a key role in supporting ESMA's digital transformation initiatives and driving information governance.

Furthermore, as a European Union agency, ESMA has to comply with the Documents, Records and Archives Management framework applicable to the EU institutions. This policy is aligned with the European Commission e-Domec (Electronic archiving and Document Management Policy of the European Commission) and Archives legal and regulatory framework for Records and Archives Management within the European Commission and EU agencies.

[1] For example, the Market Abuse Regulation 596/2014 "MAR" and Final Report Draft technical standards on the Market Abuse Regulation 28 September 2015 (ESMA/2015/1455).

4 Purpose and scope

Information is a major asset that ESMA has the duty and responsibility to protect[2]. ESMA fully recognises the benefits of managing all of its information assets in order to deliver better and more efficient services, in particular, records about business activities and transactions.

This Information and Records Management (IRM) policy mandates the creation, use and management of ESMA's information assets and records. The Authority aims to the principles set out in this policy, which supports robust decision-making, risk management and compliance with external requirements. This policy is an integral part of the overall governance of the Authority's business processes. It promotes a consistent approach to information governance within ESMA and interactions with all stakeholders and partners.

Failure to properly create, describe, capture, manage and store information could expose the organisation to increased risk and/or inhibit ESMA's ability to carry out its mission to support the standardisation, transparency and reliability of financial information to the securities markets. 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 policy will enable the integration of information governance principles and practices into ESMA's governance and business processes, in order to allow:

- optimised delivery of programmes and services;
- reuse of information for economic and social benefits;
- protection of personal data, professional secrecy and the commercial interests of financial market participants (information about which is held by ESMA), rights and entitlements of citizens, staff, stakeholders and of the Authority;
- the avoidance of effort in the loss or re-creation of corporate knowledge;
- easier access for staff to relevant and complete information;
- quicker and more accurate responses - at a lower cost - to stakeholders' requests for information,
- compliance with access to information legislation, and any legal discovery; and
- the mitigation of risks to business and reputation, through a strong focus on Data Protection, access to documents and security concerns.

This policy applies to all of ESMA's information, data, records, archives, and the business processes and systems producing and managing them, including those created or delivered by third parties on behalf of ESMA, and managed either in-house or off-site.

[2] ESMA's Information Security Policy (ESMA/2014/INT/130).

The policy covers all information and records, in both digital and non-digital format, which are created, used, received and/or distributed as part of ESMA's activity, including:

- hard copy data and documents, in print or written form;
- data stored electronically, including documents, intranet, extranet, and business systems data;
- communications sent by post, courier or by electronic means (email, voice and text messages); and
- audio and video recordings[3].

The policy aligns with ESMA's internal policies and procedures, in particular those related to Information Security, Data Protection and Access to Documents.

5 Legal and regulatory bases for ESMA's Information and Records Management

ESMA has to comply with general EU legal and regulatory requirements for documents, records and archives management. Moreover, ESMA's specific legal and regulatory bases include records and information management specific requirements.

5.1 General EU legal and regulatory requirements

The main requirements applicable to information, records and archives management at ESMA stem from the legal and regulatory EU general framework, as follows:

5.1.1 Mandatory legal and regulatory requirements

- The archives, data protection, public access regulations.
- The EC Human Resources, Finance and Internal Control, and Anti-fraud regulations.
- The Complaints to the Ombudsman and Proceedings before the Court of Justice of the EU regulation.

See detailed references in Annex 1.

5.1.2 Recommended by the European Commission to EU institutions

- The European Commission e-Domec (Electronic archiving and Document Management in the European Commission) regulatory framework (recommended for the agencies).
- The legal value of electronic documents and electronically signed internal documents (recommended to all Document Management officers).

[3] ESMA's Information Security policy (ESMA/2014/INT/130).

- The security of information systems and the interoperability solutions frameworks for European public administrations.
- The public procurement, Eco Management and Audit Scheme regulations.
- The Intellectual Property International Treaties and EC Regulation.

See detailed references in Annex 1.

5.2 Specific ESMA's legal and regulatory requirements

The specific requirements applicable to information, records and archives management at ESMA stem from:

- the ESMA's legal and regulatory framework, mainly from the ESMA's founding Regulation, in particular the articles regarding the collection of information, the use of confidential information, the protection of business secrets and other confidential information, the obligation of professional secrecy, the confidentiality of information made available to the Authority and exchanged in the network, the personal data protection, the public access to documents, the complaints to the Ombudsman and the proceedings before the Court of Justice of the EU, the Anti-fraud regulation, the Court of Auditors and OLAF investigations, and
- the Memorandum of Understanding (MoU) between ESMA and the Directorate General Human Resources and Security of the European Commission.

See detailed references in Annex 2.

6 Reference documents

6.1 ESMA's internal policies, procedures and strategic orientation

The current policy aims to support the ESMA Strategic Orientation 2016-2020[4].

It refers to and complements any ESMA policies and procedures requiring information and records management, with particular reference to internal governance, access to documents, data protection, archives, ethics and fraud prevention, security, information technology, infrastructure and work environment, and all ESMA business processes' policies and procedures.

The specific requirements for the management of information and records related to each business process will be addressed in the specific Information and Records Management (IRM) procedure.

[4] ESMA Strategic Orientation 2016-2020 (ESMA/2015/935): http://intranet.esma.europa.eu/SiteAssets/Lists/ESMA/NewForm/2015-ESMA-935%20ESMA%20Strategic%20Orientation%202016-2020.pdf

6.2 International standards

This policy is primarily based on the ISO Standard 15489-1: 2016 - Records Management. The Information Security policy and procedures are primarily based on the International Standards for Information Technology, and Information Security and Risk (ISO Standards ISO/IEC 27001/27002 (2013) on information security management systems and ISO/IEC 27005 (2011) on information security risk management).

Other ISO standards and best practices may be referred to in specific projects, such as ISO20020 for the IT Delegated Projects.

7 Policy statements

7.1 General requirements for information and records management at ESMA

ESMA is an independent Authority, but is accountable to the European Parliament, the Council of the European Union and the European Commission.

In line with its mission and objectives, ESMA aims to creating and keeping accurate and reliable records of its activity. Several objectives of ESMA are directly related to the management of information, its collection, protection and publication.

ESMA's information and records are a corporate asset, vital for ongoing operations and for providing valuable evidence of business decisions, activities and transactions.

ESMA aims to supporting the legal requirements resulting from EU regulations and recommendations, in addition to its own policies.

Since 2011, ESMA laid the foundations of its Information and Records governance by setting up a series of foundational policies and tools, such as Access to documents and Data Protection Decisions (in 2011) and a set of Information Security policies and procedures (in 2014). The current objectives of this policy are to **focus on information and documents security (secrecy and confidentiality), traceability, search ability**. The supporting **procedure** should be **transparent and traceable** to ensure that the Authority meets its **stakeholders' expectations for accountability**. In meeting these objectives, the Authority faces new challenges and opportunities, which it must incorporate:

- "Put in place and maintain an effective document management system so that any document connected with ESMA's official functions can be electronically filed, stored and retrieved in any moment, irrespective of its original form and the document management system in place" (see 2012 internal control audit finding concerning Internal control standards).
- Permanent audits (European Court of Auditors, ex post controls, etc.) and the need to produce evidence-based information to authorities.

- The need to manage multiple information streams, both in paper and digital format, such as webmail and internal notes, business processes or data processing outputs, intranet and internet, etc. throughout the entire information and document life cycle, from creation to archiving or disposal, taking into account all legal and business requirements.
- The need to federate the search in ESMA's different information streams via user-friendly and easy to search, intuitive tools.
- Increasing digitization of business processes, with a need for certainty and authenticity[5].
- Beyond managing documents, the need to take on board the business processes data and information, databases and emails, in order to preserve evidence of business activity.
- The need to establish an archiving policy for the management of both paper and electronic archives and, at the same time, to implement the new Council Regulation (EU) 2015/496 of 17 March 2015 regarding the institutions and agencies historical archives.

7.2 Principles for ESMA's Information and Records governance

This policy defines the requirements for the effective and secure management of ESMA's information and records (both in paper and electronic format) throughout the entire information life cycle, while taking into account legal issues, security, stakeholders and other business requirements.

The objective is the creation, capture and management of authentic, reliable and useable records that possess integrity and support and enable business activity for as long as they are required.

ESMA's Information and Records Management principles are:

- ESMA's governance mechanisms, policies and procedures ensure that information management practices support good decision-making with integrity, accountability and transparency to deliver high-quality services. Business information and records provide a reliable and accurate account of business decisions and actions. Our information is authentic, accurate, up to date and complete (and this can be demonstrated).
- Personal information is fairly and lawfully processed for limited purposes; adequate, relevant and not excessive; accurate and up to date; not kept for longer than necessary; secure and processed in line with a person's rights and entitlements.
- Commercial interests of financial markets participants (information about which is held by ESMA) are protected, in accordance with the obligation of professional secrecy in Article 70 of ESMA's Regulation.

[5] See Financial regulation and Rules of Application, ISA and eIDAS Regulation EU No 910/2014.

- Records include all necessary information to support business processes and evidential needs including the names, dates and time, business/activities classification and other key information needed to capture the business context.

ESMA's information and records shall possess the following characteristics and attributes: authenticity, reliability, integrity, usability and appropriate metadata. These essential records attributes can be summarised as below:

a) **Authenticity**: the record can be proven to be what it purports to be, to have been created or sent by the person that created or sent it, and to have been created or sent at the time it is purported to have occurred.
b) **Reliability**: the record can be trusted as a full and accurate representation of the transaction(s) to which they attest, and can be depended on in the course of subsequent transactions.
c) **Integrity**: the record is complete and unaltered, and is fixed. This characteristic is also referred to as 'inviolability'.
d) **Usability**: the record can be located, retrieved, preserved and interpreted.
e) **Metadata** for records should depict the following:
    i. business context;
    ii. dependencies and relationships among records and records systems;
    iii. relationships to legal and social contexts;
    iv. relationships to agents who create, manage and use records.

For this purpose:

- ESMA aims to draft records classification and procedures and controls to link the business processes/systems and the records, based on business process analysis (including data protection and confidentiality requirements).
- All business information and records created and received are captured into endorsed information and records systems, unless they can be disposed of, according to an authorised retention and disposition schedule.
- Information is discoverable across the Authority, accessible and available for re-use, to those with a valid need and access right.
- It is available for as long as needed and deleted/transferred to archives when necessary.
- ESMA's systems protect information (especially personal data, business secrets and other confidential information) from unauthorised access, against alteration, deletion or misuse.
- ESMA's staff understand and appreciate the value of information as an asset for the organisation; that information is required as evidence of ESMA's activities, is managed in alignment with citizens' rights, and forms part of the historical and cultural heritage of the Authority and of the EU. Business information and records are created and captured by everyone who is subject to this policy as defined in section 8 (Responsibilities).

7.3 Requirements for managing information and records

7.3.1 Decentralised functional organisation

Information and Records Management is decentralised across ESMA. Each department and business process (data) owner aims to implement the information and records requirements hereby, and to ensure they are regularly met, maintained and improved.

7.3.2 Sharing corporate information and records within ESMA

Information and records are a corporate resource. Access restrictions protect:

- The privacy of staff members and stakeholders;
- the commercial interests of financial market participants (information about which is held by ESMA), in accordance with the obligation of professional secrecy in Article 70 of ESMA's Regulation; and
- sensitive material, marked as "ESMA restricted use" and "ESMA confidential use", according to the Data Classification policy (ESMA/2014/INT/134) or bearing dissemination limiting markers.

When handling information, staff are reminded of their obligations under the applicable regulations and internal policies (see above sections 4 and 5 and annexes 1, 2 and 3).

The data classification status of each process will be assessed within the business process analysis. Accurate rules will be set and recorded in the filing, classification, data protection and retention procedures and database.

7.3.3 Release of publicly available information

In accordance with ESMA's obligations under the Regulation (EC) No 1049/2001 regarding public access to documents, access to publicly available information is provided on ESMA's public registers databases and library, on ESMA's website. The publication and release of this information falls under the responsibility of the Communications team (CAD Department), while ensuring its accuracy lies with the relevant departments within the organisation i.e. those with responsibility for relevant databases, maintenance of lists, and production of policy documents.

Additionally, the public has a series of legal rights to request access to information held by ESMA, according to the same Regulation (EC) No 1049/2001 and ESMA's Decision on Access to documents (ESMA/2011/MB/69). This applies to all information held by the Authority, whether it is stored in officially endorsed records management systems or in computer folders that are personal or shared. Responding to such requests for access under this regulation falls under the responsibility of the Document Access Coordinator (in LCE - regarding initial applications) and the Executive director (regarding confirmatory applications).

7.3.4 Retention and destruction

Staff responsibility for the retention and authorised destruction of ESMA's information and records includes their timely disposal, according with data protection and classification regulations and requirements. It avoids any risks stemming from unauthorised destruction.

ESMA's records should be destroyed when they reach the end of the required retention period, as set out in the filing, classification, data protection and retention procedures and database. The retention period takes into account that all legal and business requirements for the records have been met. For this purpose, ESMA aims to draft records retention procedures and controls to determine precisely what the retention, destruction and transfer actions for its records will be, based on business process analysis.

However, some records of short-term, facilitating or transitory value may be destroyed routinely in the course of business as a 'normal administrative practice'. Examples of such records include rough working notes, drafts not needed for future use or copies of records held for reference.

Staff should only destroy records in accordance with the authorised procedures, and should be aware that unauthorised destruction may expose ESMA to risks, including:

- The inability to comply with regulatory and legislative responsibilities;
- the inability to provide access to information requested by legal discovery action; and
- damage to corporate reputation.

7.3.5 Transfer

At the end of the required retention period, records may require to be transferred. In particular, records with archival value are required to be transferred to ESMA's archives, and then to the EC Historical Archives, once they are no longer needed for current use.

Staff will still be able to access records where a subsequent need arises.

An ESMA's archives policy will form the final part of the ESMA information governance framework.

7.4 Requirements for business processes and systems

7.4.1 Business processes

Information is produced and maintained in the course of ESMA's business, and ESMA's business processes are increasingly supported by systems and technology. Key information requirements in business processes are represented mainly by:

- Good metadata
- Interoperability

- Accessibility
- Data quality

Detailed Information and Records Management requirements relevant to each business process and system will be described in the Information and Records Management procedure, which will be based on a business process analysis.

7.4.2 Systems

ESMA's enterprise architecture supports current and future missions of the Authority by continuing to meet its obligations whilst maintaining a good level of quality and service, a good time to market and a reasonable cost.

ESMA's enterprise architecture includes:

- Applications Architecture
- Business Architecture
- Data Architecture
- Technology Architecture

Enterprise architecture governance is based on principles and orientations.

A catalogue and maps of applications, businesses, data and technologies allow identifying, assessing and documenting ESMA's business systems and data. It is made available and maintained by the ICT Architecture team. See details in Annex 4.

This is not limited to business systems owned and maintained by ESMA or located in ESMA's premises. This extends to systems and technology hosted in the cloud, via social media and mobile devices.

All the business and administrative databases and software applications should meet the requirements for the capture and storage of specific information and records as set out in this policy and in the relevant procedures. These endorsed systems should comply with the Information and Records Management requirements, such as creation and capture, classification, storage, protection of integrity and authenticity, security, access and retention, destruction and transfer.

7.4.3 ESMA's electronic documents and records management system

SHERPA (MS SharePoint-based document management system) is the major tool to be used for documents creation, co-authoring, sharing and search within ESMA. So all records (documents and emails) should be created, registered and managed in SHERPA. The main metadata will be captured (as much as possible automatically) in SHERPA, according to Information and Records Management controls.

Corporate records must not be maintained in email folders, shared folders, personal drives or external storage media as these lack the necessary functionality to protect business information and records over time (except for confidential matters, according to applicable internal procedures) . Records created when using social media applications or mobile devices may need to be captured into an endorsed system.

The use of ESMA's former shared folders is maintained, but provides only limited access to the 2011-2015 documents (see above 7.3.5 – Transfer).

Wherever possible, incoming paper correspondence received by the Authority is converted into digital format and saved into the Electronic Document and Records Management System (EDRMS). In limited circumstances, such as for particular security purposes, there may be a requirement for paper files to be created (according to specific procedures).

8 Responsibilities

8.1 Senior Management

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

Accountability and transparency are at the core of ESMA's mission. ESMA's Executive Director has overall responsibility for how information is managed and used within the organisation.

ESMA Senior Management promotes compliance with this policy and delegates responsibility for the operational planning and running of Information and Records Management to the Head of the Resources Department.

8.2 Head of the Resources Department

The Head of the Resources Department is responsible for the operational planning and running of the information and records management programme, and ensures that it is adequately resourced.

He/she is also responsible for promoting Information and Records Management, as well as the convergence strategy with IT, security, data protection and ESMA's policies (in collaboration with the Head of the Legal, Convergence and Enforcement Department).

8.3 Management

Managers are responsible for the visible support of, and adherence to this policy, by promoting a culture of compliant information and records management within the Authority and by contributing to the development of strategic documents, such as the Information and Records Management framework and strategy.

They aim to integrate the Information and Records Management requirements in the business processes and business systems under their responsibility.

Managers are also responsible for ensuring that staff, including outsourced staff, are aware of, and are supported to follow the Information and Records Management (IRM) policy and procedure. They should inform the Information and Records Management Officer of any barriers that staff might be confronted with in complying with this policy. They should also advise him/her of any changes in the business environment that would have an impact on the Information and Records Management requirements, such as new business areas that need to be covered by a records procedure.

8.4 Information and Records Management Officer

Under the leadership of the Head of the Resources Department, the Information and Records Management Officer will be appointed, once resources will be available. He/she is responsible for overseeing the management of information and records consistently with the requirements described in the policy. This includes:

- Developing and implementing strategies to enable sound information and records management practices, monitoring compliance with information and records management policies and directives, and advising Senior Management of any risks associated with non-compliance.
- Developing and maintaining Information and Records Management policies and procedures in collaboration with managers and officers from Legal, Data Protection, Security and IT areas, and with the SHERPA Project Manager.
- Developing, implementing and maintaining metadata schemes and other controls, in association with other personnel, such as information technology professionals, business managers, Legal, Data Protection and Security professionals.
- Ensuring that Information and Records Management products and tools are developed or acquired and implemented, including the designing, implementation and maintenance of records systems and their operations so that complete and accurate records are produced.
- Ensuring that communication, training, advice and general support to staff is available as needed.

8.5 Staff with special responsibilities

Staff members with special responsibilities linked to the Information and Records Management are listed below:

- The Legal and Data Protection Officers, Security Officer, Head of ICT Unit, ICT Senior Architect, Business Process Owners and the SHERPA Project Manager are responsible for participating in developing and maintaining the Information and Records Management policies and procedure (in collaboration with the Information and Records Management Officer).

- The **Security Officer, Head of ICT Unit,** ICT Senior Architect, ICT Officers, **Business Process Owners and the SHERPA Project Manager** are responsible for maintaining ESMA's business information and records systems, including maintaining an appropriate system accessibility, security and back-up. ICT Officers should ensure that any actions, such as removing data from ESMA systems or folders, are undertaken in accordance with this policy. ICT Officers and Business Process Owners, together with the Information and Records Management Officer play an important role in ensuring that ESMA's IT systems support accountable and effective information and records management across the organisation.
- The **Security Officer** ensures that security requirements are incorporated in the IRM policies and procedure**.** He/she also gives advice on security issues associated with the management of information.
- The **Legal Officer and the Data Protection Officer** ensure that the Legal and Data Protection requirements are incorporated in the IRM policies and procedure. They also give advice on legal and data protection issues associated with the management of information.
- The Facility Management (FM) Team Leader together with the FM team is responsible for the physical storage of (paper) archives and vaults, cupboards and other furniture, especially security and access. He/she is also, with the Post Officer, responsible for the handling of paper mail.

8.6 Staff members

All staff members are responsible for the production and management of information and records as defined by this policy, particularly to ensure that reliable and useable information and records are generated, managed and kept for as long as they are needed for business, accountability or historical purposes.

This policy applies to the persons described in Article 70(1) of the ESMA Regulation, including all personnel affiliated with third parties who have access and use ESMA's information systems.

9 Strategy, organisation and planning

Information and Records Management (IRM) will be integrated into the Authority's strategies and planning requirements. This involves incorporating IRM requirements in ICT, Security and Data Protection areas, in its strategies and policies, and in all ESMA's future policies and procedures.

Development and implementation

ESMA aims to develop the procedures required to complement this policy. This includes the drafting of the Information and Records Management procedure. Concurrently, the requirements for Electronic and Document Records Management services (EDRMS) to be

incorporated in business systems will be identified, so that such services may be implemented in the future.

Monitoring and review

This policy, the IRM procedure and the whole Information Governance framework should be periodically reviewed to ensure that they are accurate and up to date. Additionally, the framework should be reviewed after any events that might affect information management arrangements, such as major business or regulatory changes.

10 Risk management and audit

This policy is part of ESMA's approach to risk management. Proper management of information helps to reduce the risks, while a robust risk management framework helps to protect information. IRM controls will ensure adequate protection of information assets.

External audits to which ESMA is subject (for example: from the Internal Audit Service and the European Court of Auditors) may include items related to Information and Records Management.

11 Communication and training

All staff must be aware of the Information and Records Management framework and kept up to date with any subsequent changes.

The approved policy will be published on ESMA's intranet.

12 Consultation status

Prior to its approval, this policy 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.

13 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).

14 Records

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

15 Final provisions

This policy will enter into force on 18/04/2017.

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

16 ANNEX 1 - General EU Legal and Regulatory bases for ESMA's Information and Records Management requirements

16.1 Mandatory legal and regulatory requirements

Archives:

- Council Regulations (EU) 2015/496 of 17 March 2015 and 1700/2003 amending Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the EC Historical Archives of the European Economic Community and the European Atomic Energy Community.

Data Protection

- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Public access

- Regulation (EC) No 1049/2001 of the European Parliament and of the Council, regarding public access to European Parliament, Council and Commission documents. Commission Decision 2011/833/EC, Euratom, on the reuse of Commission documents.

Complaints to the Ombudsman and Proceedings before the Court of Justice of the EU
Articles 228, 263. 265 and 340 of the Treaty on the Functioning of the European Union.

Human Resources

- Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45, 14.6.1962, p. 1385).

Finance and Internal Control

- Regulation (EU, EURATOM) No 966/2012 on the financial rules applicable to the general budget of the Union and its rules of application (Commission delegated regulation EU No 1268/2012).

In particular:

Article 66 (Powers and duties of the authorising officer) and related Rules of application (RAP). Article 48 (Keeping of supporting documents by authorising officers), and FR 93 to 95 and related RAP Articles 112 and 113 (Chap. 7: IT systems and e-Government).

The Internal Rules (Commission Decision C (2015) 1423 final) lay down the rules to be applied by the Commission and the executive agencies and in article 16 the rules regarding documents and signature are explained.

- Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework Financial Regulation.
- Commission Regulation (EC, Euratom) No 2343/2002 of 19 November 2002 on the framework Financial Regulation for the bodies referred to in Article 185 of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities.

Anti-fraud

- Regulation (EC) No 1073/1999 Inter institutional Agreement concerning internal investigations by OLAF.

16.2 Recommended by the European Commission

- **European Commission e-Domec (Electronic archiving and Document Management in the European Commission) regulation**[6]) Communication to the Commission C(2002)99 - Simplification and modernisation of the management of the Commission's documents (Action 9 of the interim action plan on simplification).
- Commission Decision 2002/47/EC, ECSC, Euratom.
- Commission Decision 2004/563/EC, Euratom (Provisions on electronic and digitised documents DOCELEC)[7].

Legal value of electronic documents and electronically signed internal documents

- European Commission SG.B.1-Corporate Management, Budget and Administration: Ares (2015)2641903 - 24/06/2015: “Legal bases for all electronic documents”

1. Financial regulation: Regulation (EU, EURATOM) No 966/2012 and its rules of application (Commission Delegated regulation (EU) No 1268/2012).

[6] “Legal framework for records management in the EU agencies” Version 1.0, Philipp Wilhelm (EEA), with edits from Josefus Schram, Robert Stowell, Marc Willem, 22 March 2016.
[7] NB: A work in progress of the legislative framework, aims to broaden the scope to the whole data and information managed by the Commission and its agencies, with a strong concern for data protection. Draft Communication of the Commission to the College (Sept 2016) and project of Commission policy for data, information and knowledge management.

Article 66 (Powers and duties of the authorising officer) and related Rules of application (RAP) Article 48 (Keeping of supporting documents by authorising officers), and FR 93 to 95 and related RAP Articles 112 and 113 (Chap. 7: IT systems and e-Government).
The Internal Rules (Commission Decision C2015- 1423 final) lay down the rules to be applied by the Commission and the executive agencies and in article 16 the rules regarding documents and signature are explained.

2. Commission decision 2004/563/EC (articles 4 and 5) and its implementing rules SEC (2009)1643 for the provisions on electronic and digitised documents (III.2.1 – III.2.4).

3. Directive 1999/93/EC on the community framework for e-signatures and regulation EU No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC.

Security

- Commission Decision 2001/844/EC, CECA, Euratom of 29 November 2001, Commission decision C(2006) 3602 on Security of Information Systems; Implementing Rules (EN) for Commission Decision C(2006) 3602; Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission.

ISA: Interoperability solutions and common frameworks for European public administrations

- Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a mean for modernising the public sector (Text with EEA relevance).
- **Including: Electronic Identification (eID) and Electronic Trust Services (eTS)** Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014[8].

Public Procurement

- Directive 2014/24/EU on public procurement.
- Directive 2014/25/EU on procurement by entities operating in the water, energy, transport and postal services sectors.
- Directive 2014/23/EU on the award of concession contracts.

In the framework of Public Procurement, the Commission has developed e-PRIOR, an open-source e-procurement platform that allows practical implementation of interoperable electronic

[8] Note: On 8 September 2015, the European Commission completed the adoption of all the implementing acts due by 18 September 2015.

services within any public administration. It is already used by many EC services and ESMA may join this platform.

Eco Management and Audit Scheme

- Revised Regulation (EC) No 1221/2009 of the European Parliament and of the Council of 25 November 2009 on the voluntary participation by organisations in a Community eco-management and audit scheme (EMAS III).
- Decision C/2009/6873 on the application by the Commission services of the Community eco-management and audit scheme (EMAS).

Intellectual Property[9]

- International treaties:
  - Berne Convention for the Protection of Literary and Artistic Works (1886).
  - National IP laws of the EU Member States.
- EC regulations:
  - Commission Decision 2011/833/EU of 12 December 2011 on the re-use of Commission documents http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0833
  - Communication to the Commission SEC (2012)103 of 16 February 2012 towards a more effective management of Intellectual Property Rights at the European Commission
  - Communication to the Commission SEC (2005)1327 of 20 October 2005 towards an effective and coherent risk management in the Commission Services.
  - Directive 96/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases.
  - Octroi de Pouvoirs Délégués SEC(2001)1397 du 12 Septembre 2001 dans le domaine de la Propriété Intellectuelle (Délégation aux Directeurs Généraux et Chefs de Services)[10].

[9] Excerpt from Annex c of *"Standard Operating Procedures on the Effective Management of IPR at the Commission" [Communication SEC (2012) 103]:* https://myintracomm.ec.testa.eu/serv/en/intellectual-property/Documents/IPR%20Vade%20Mecum%20v1.0.pdf

[10] *"Guidelines on the Rights and Duties relating to Literary, Scientific and Artistic Works produced by the staff members of the European Commission". Also, see: http://ec.europa.eu/ipg/basics/legal/notice_copyright/index_en.htm and* http://ec.europa.eu/ipg/about/rules/index_en.htm#section_1. Also : EC web site Legal Notice http://ec.europa.eu/geninfo/legal_notices_en.htm

17 ANNEX 2 - ESMA's specific legal and regulatory bases for Information and Records Management requirements

ESMA's Establishing Regulation (*Mandatory*)

- Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC. Amended by:
- Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011.
- Directive 2014/51/EU of the European Parliament and of the Council of 16 April 2014.

In particular:

- Recitals 61 (open and transparent employment conditions), 62 (protection of business secrets and other confidential information, confidentiality of information made available to the Authority and exchanged in the network), 63 (personal data protection), 64 (public access to documents).
- Article 4 (ESFS "Ensuring the flow of appropriate and reliable information").
- Article 8 (Tasks and powers of the Authority): "(k) publish on the Authority's website and update regularly, information related to its field of activities (…) in order to ensure information is easily accessible by the public), (h) collect the necessary information concerning financial market participants (…), (j) provide a centrally accessible database of registered financial market participants in the area of its competence (…)".
- Article 21 (a) "collect and share all relevant information in co-operation with the competent authorities in order to facilitate the work of the college and establish and manage a central system to make such information accessible to the competent authorities in the college".
- Article 29 (b) "promoting an effective bilateral and multilateral exchange of information between competent authorities, with full respect for the applicable confidentiality and data protection provisions provided for in the relevant Union legislation".
- Article 31 (coordination function between NCAs), a, b and f (exchange of information, reliability of information, centralising and sharing information).
- Article 35 (Collection of information, use of confidential information).
- Article 36 (ESRB) 2. "The Authority shall provide the ESRB with regular and timely information (…). Any data necessary for the achievement of its tasks that are not in summary or aggregate form shall be provided, without delay, to the ESRB upon a reasoned request (…). The Authority, in co-operation with the ESRB, shall have in place adequate internal procedures for the transmission of confidential information, in particular information regarding individual financial market participants."

- Article 39 (Decision-making procedures): “inform any named addressee of its intention to adopt the decision (…), setting a time limit within which the addressee may express its views on the matter (…)”.
- Article 66 (Anti-fraud regulation, Court of Auditors and OLAF investigations).
- Article 70 (Obligation of professional secrecy): “2. Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial market participants cannot be identified. Moreover, the obligation under paragraph 1 and the first subparagraph of this paragraph shall not prevent the Authority and the national supervisory authorities from using the information for the enforcement of the acts referred to in Article 1(2), and in particular for legal procedures for the adoption of decisions. 3. Paragraphs 1 and 2 shall not prevent the Authority from exchanging information with national supervisory authorities in accordance with this Regulation and other Union legislation applicable to financial market participants”. That information shall be subject to the conditions of professional secrecy referred to in paragraphs 1 and 2. The Authority shall lay down in its internal rules of procedure the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.
- Article 71 (Data Protection).
- Articles 72 (Access to documents, Complaints to the Ombudsman and Proceedings before the Court of Justice of the EU) (Mandatory).

Memorandum of Understanding (MoU) between ESMA and the Directorate General Human Resources and Security of the European Commission.

18 ANNEX 3 - ESMA's policies and procedures requiring Information and Records Management

This annex provides a list of the current ESMA's policies and procedures requiring Information and Records Management, as identified when drafting this document.

ESMA Strategic Orientation 2016-2020[11] (see ESMA/2015/935, page 18: "*Strengthen core administrative processes: we will further increase the quality of ESMA's core administrative processes. This includes our IT support systems, internal and external registries and databases, filing systems, general management systems*."). Any ESMA policies and procedures requiring information and records management (see ESMA's process map of policies and procedures[12], with particular reference to:

Internal Governance

- ESMA Internal Control Standards (ESMA/2012/MB/62 Annex 2 (rev 2): Part IV (Operation and Control Activities, including §11 – Document Management), Part V (Information and Financial Reporting) and Part VI (Evaluation and Audit)[13].
- Decision on Code of good administrative behaviour (ESMA/2011/MB/6)[14].

Access to documents

- Decision on Access to documents (ESMA-2011-MB-69)[15].

Data Protection

- Decision on Data Protection implementing rules (ESMA/2011/MB/57)[16].

Archives

- Policy about ESMA's Archives (based on Council Regulation (EEC, Euratom) No 354/83, amended by Council Regulation (EU) 2015/496 of 17 March 2015, concerning the opening to the public of the historical archives of the EU).

[11] https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-935_esma_strategic_orientation_2016-2020.pdf
[12] http://intranet.esma.europa.eu/Policies%20and%20procedures/Pages/default.aspx
[13] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Governance/Internal%20governance/2012-MB-62%20Annex%202%20(rev%202)%20-%20ESMA%20Internal%20Control%20Standards.pdf
[14] https://www.esma.europa.eu/sites/default/files/library/2015/11/2011_mb_6.pdf
[15] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Access%20to%20documents/ESMA-2011-MB-69%20-%20Decision%20on%20access%20to%20documents%20rules.pdf
[16] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Data%20protection/ESMA-2011-MB-57%20-%20Decision%20on%20Data%20protection%20implementing%20rules.pdf

Ethics and fraud prevention

- Decision on Professional secrecy (ESMA/2011/MB/4)[17].
- Decision on Anti-fraud measures (ESMA/2011/MB/5)[18].

Security

- Information Security policy (ESMA/2014/INT/130)[19].
- Information Security Acceptable Use policy (ESMA/2014/INT/131)[20].
- Identity and Access Management policy (ESMA/2014/INT/132)[21].
- ESMA's Security Governance policy (ESMA/2014/INT/133)[22].
- Data Classification policy (ESMA/2014/INT/134)[23].
- Data Retention and Disposition policy (ESMA/2014/INT/136)[24].

Information Technology

- ESMA IT Strategy 2016-2020[25], page 18: "Strengthen core administrative processes: we will further increase the quality of ESMA's core administrative processes. This includes our IT support systems, internal and external registries and databases, filing systems, general management systems.").

Infrastructure and work environment

- Registering incoming emails (ESMA/2015/INT/7)[26].

---

[17] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Ethics%20and%20fraud%20prevention/ESMA-2011-MB-4%20-%20Decision%20on%20Professional%20secrecy.pdf

[18] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Ethics%20and%20fraud%20prevention/ESMA-2011-MB-5%20-%20Decision%20on%20Anti-fraud%20measures.pdf

[19] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Security/ESMA-2014-INT-130%20-%20Information%20Security%20policy.pdf

[20] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Security/ESMA-2014-INT-131%20-%20Information%20Security%20Acceptable%20Use%20policy.pdf

[21] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Security/ESMA-2014-INT-132%20-%20Identity%20and%20Access%20Management%20policy.pdf

[22] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Security/ESMA-2014-INT-133%20-%20ESMA's%20Security%20Governance%20policy.pdf

[23] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Security/ESMA-2014-INT-134%20-%20Data%20Classification%20policy.pdf

[24] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Cross-cutting/Security/ESMA-2014-INT-136%20-%20Data%20Retention%20and%20Disposition%20policy.pdf

[25] https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-935_esma_strategic_orientation_2016-2020.pdf

[26] http://intranet.esma.europa.eu/Policies%20and%20procedures/Documents/Infrastructure%20and%20work%20environment/Facility%20management/ESMA-2015-INT-7%20-%20Work%20Instruction%20Registering%20incoming%20emails.pdf

19 ANNEX 4 - IT systems