Information Management Policy

Special Requirements	This procedure is a controlled document maintained by Quality Management. It may not be deleted without comparable controls. Please note that this document becomes uncontrolled once printed. Make sure by always referring only to the Repository that you have the right version in use. Deviations from the provision of this document need to be recorded in the Exception Request Workflow. The procedure should be updated when there are changes in EFSA with respect to what is stated in the document (e.g., Relevant Standards, legislation, and documents, change in procedure, etc.). The person responsible for maintaining this procedure up to date is the Lead author with the support of the QM.

Process Responsibility	Process owners are accountable this procedure being adhered to within their respective or unit. All relevant staff is responsible for the correct implementation of the procedure. Responsibilities for performing specific steps are outlined in the document.

Introduction

This policy sets out an overarching framework for information management in EFSA, underlining EFSA's commitment to achieving high standards in Records Management (RM), the Data Protection dimension in Information Management, Information Security, and in fulfilling Historical Archive obligations. It also gives guidance on information security categorisation.

Record Management is an essential aspect of information management, vital to the delivery of EFSA's services in an orderly, transparent, efficient, and accountable manner. Effective record management will help ensure that EFSA has the right information at the right time to make the right decisions.

To comply with the legal and institutional framework within which EFSA operates, all documents and data sets produced or received by the Agency must be systematically and efficiently managed in a legally compliant manner throughout their entire lifecycle, i.e. from their creation and labelling as a record until their destruction or permanent archiving. Uniform record-keeping practices are fundamental to supporting proper implementation of EFSA's Accountability pillars i.e. Governance and decision-making, Results—based management, Assurance and Quality Management; and more specifically to:

- help fulfil transparency obligations and good administrative practices, while ensuring correct information classification;
- enhance business continuity, knowledge retention, efficiency and information security; facilitating access to corporate knowledge by enabling staff members to find with minimum delay and effort information required for their work;
- ensure compliance with legal obligations including in the area of personal data protection and historical archiving.

Capturing EFSA's records into the appropriate Records Management System (RMS) is vital to link the record, its creator and the business context in which it originated. It is also vital to track the access, the record modifications (versioning), and to check permissions.

An important aspect of the Policy is to ensure compliance of personal data handling in EFSA's information management and processes with Regulation (EU) 2018/1725 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, as well as with relevant internal rules applicable at EFSA, including SOP 38.

The Policy will be supported through the delivery of standards and procedures, primarily by means of Standard Operating Procedures (SOPs).

Scope and principles

This Policy covers all information, documents and data sets (hereafter Documents) created or received by EFSA in the course of its operational or administrative processes and activities, providing guidance on the classification of Documents or Data as Records, and providing guidance on information security categorisation and/or personal data protection requirements.

Specifically regarding Records, the following principles apply:
- EFSA shall organise its Records according to common rules in order to retrieve information quickly and efficiently in the course of its internal and external collaborative activities, in compliance with the usability principle.
- EFSA must be able at any time to provide reliable, authentic and complete Records on the matters for which it is accountable.
- Records shall be declared into the appropriate RMS for EFSA to provide evidence of its institutional or legal obligations, or in the transaction of its business.

This Policy applies to *EFSA staff in a broad sense*, i.e. statutory staff, non-statutory workforce, and any external agents (e.g. contractors and consultants, external experts) who take part in EFSA's processes and activities.

References

Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing EFSA and laying down procedures in matters of food safety OJ L 31, 1.2.2002, p. 1–24., hereunder referred to as '*the General Food Law Regulation*'

Regulation (EU) 2019/1381 of the European Parliament and of the Council of 20 June 2019 on the transparency and sustainability of the EU risk assessment in the food chain and amending Regulations (EC) No 178/2002, (EC) No 1829/2003, (EC) No 1831/2003, (EC) No 2065/2003, (EC) No 1935/2004, (EC) No 1331/2008, (EC) No 1107/2009, (EU) 2015/2283 and Directive 2001/18/EC, PE/41/2019/REV/1, OJ L 231, 6.9.2019, p. 1–28.

Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, p. 43-48, applicable to EFSA, hereunder referred to as '*the PAD Regulation*'.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98, hereunder referred to as '*the Data Protection Regulation*'.

Staff Regulations of Officials to the European Communities, Title II, i.e. art 17 to 19: staff members may not purposefully disclose confidential or sensitive information within or outside the authority, except to individuals known to be authorized to receive such information and staff members should take due regard of the intellectual property of the Union concerning the deliverables and outputs of their assigned tasks.

Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, OJ L 193, 30.7.2018, p. 1–222

Council Regulation (EC) No 354/83 Concerning the opening to the public of the Historical archives of the EEC and the EAE Community, amended by Council Regulation (EC, EURATOM) No 1700/2003 and by Council Regulation (EU) No 2015/496, OJ L 43, 15.2.1983, p. 1–3.

Commission Decision (EU) 2021/2121 of 6 July 2020 on records management and archives.

The European Code of Good Administrative Behaviour

EFSA Code of Good Administrative Behaviour

EFSA Internal Control Standards Framework of 01 January 2018 (mb171212-a5)

EFSA Quality Management Policy (EFSA/SCER/POL/1589/4146/2016)

ISO 9001:2015 Quality Management Systems

ISO 14001:2004 Environmental Management

ISO 15489:2016 Information and documentation

ISO 30300:2011 Information and documentation-Management systems for records - Fundamentals and vocabulary

ISO 30301:2011 Information and documentation-Management systems for records - Requirements

ISO 30302:2015 Information and documentation-Management systems for records - Guidelines for implementation

ABBREVIATIONS AND DEFINITIONS	
Authenticity	The quality that documents are genuine and free from tampering. An authentic document is one that can be proven (a) to be what it purports to be, (b) to have been created or sent by the person purported to have created or sent it, and (c) to have been created or sent at the time purported.
Confidentiality	Confidentiality means that information is only disclosed to authorised individuals, entities or stakeholders in processes. Within this context, for example, confidential sections of dossiers for the authorisation of regulated substances should only be disclosed to EFSA staff and external stakeholders that need access in order to perform their assigned tasks.
Disposal	A disposal action is taken when the agreed period of time for which a *record* must be kept has expired, and it leads to either its destruction or its permanent preservation.
DMC	Document Management Correspondent.
DMF	Document Management Function.
Document	A document is defined as being "Any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) concerning a matter relating to the ***policies, activities and decisions*** falling within the institution's sphere of responsibility"[1].
File	A "file" is an aggregation of records organised in line with EFSA's activities, for reasons of proof, justification or information and to guarantee efficiency in the work; the group of records making up the file is organised in such a way as to form a coherent and relevant unit in terms of the activities conducted by EFSA. Not to be confused with the term "file" that is used in IT systems to describe an individual document.
Filing plan	A filing plan is an instrument with a hierarchical and logical structure, in the form of a tree structure with a number of interlinked headings, which enables files (or other aggregations of records) to be intellectually organised and linked to the context in which they were drawn up, on the basis of the functions, activities and working processes.
Historical archives	Group of operations and processes needed to store and preserve information of historical or research value for a long period of time ensuring its authenticity, integrity and usability, as per Council Regulation (EU) 2015/496 of 17 March 2015 amending Regulation (EEC, Euratom) No 354/83.
HoU	Head of Unit.
Integrity	Integrity means that the accuracy and completeness of information shall be safeguarded. In the context of Records Management this also means that a record should be complete and unaltered.
Need-to-know	Need-to-know means that an individual requires the specified information for the fulfilment of his or her official duties for EFSA (See Annex 2 of this policy).

---

[1] Article 3(a) of the PAD Regulation.

Preservation	Preservation means all technical processes and operations which make it possible to keep records over time, to maintain their integrity and authenticity and to guarantee access to their content.
Record	A record is "information, received and created in the form of a document, a collection of data or other form in a digital or analogue medium that is captured in an official repository and managed and maintained as evidence and as an asset"[2]. Records must be[3]: • Authentic • Reliable • Have integrity • Useable
Record Owner	The process manager/process owner of the relevant EFSA process, project or other activity.
Record Management System (RMS)	Electronic system designed to capture, maintain and retrieve records while ensuring their continued integrity with appropriate evidential characteristics.
Registration of documents	'Registration' means capturing a record into a Record Management System (See EFSA's "IT System Catalogue" (Annex 4)), establishing that it is complete and properly constituted from an administrative and/or legal standpoint.
Reliability	Trusted contents which accurately reflect the business transaction documented.
Retention schedule	Governance document determining the length of time that *records* should be kept in EFSA's RMSs, and their related *disposal*.
Security Classification	A way of assessing information and documents based on the likely consequences and harm of unauthorised disclosure for the interests of EFSA, the Commission, other EU Institutions or agencies, the EU Member States or other 3rd parties. There are three levels of security classification at EFSA: 1. **Public**: Information handled by EFSA that is published or ready to be published. 2. **Sensitive**[4]: Information or documents that EFSA must protect because of legal obligations laid down in the Treaties or in legal acts adopted in implementation thereof, and/or because of its sensitivity[5]. 3. **Internal**: When the information handled by EFSA is not for the public but is not sensitive either, it shall be treated as EFSA internal information[6].

---

[2] Commission Decision (EU) 2021/2121 on records management and archives, Article 3(1)

[3] ISO 15489-1:2016 (Information and documentation – Records management).

[4] In line with Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission, EFSA information may be sensitive but cannot be considered as EU classified information (EUCI). The EFSA security classification "Sensitive" is therefore the equivalent of the EC's "Sensitive Non-Classified (SNC)" security classification.

[5] Sensitive information includes, but is not limited to, information or documents covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests to be protected in application of Article 4 of the PAD Regulation read in conjunction with the relevant case-law of the Court of Justice of the European Union, categories of personal data within the scope of Article 10 of the Data Protection Regulation (e.g. health-related personal data) or confidential data within the scope of the General Food Law Regulation as amended by Regulation (EU) 2019/1381.

[6] Full or partial confidentiality of internal information and documents is established case-by-case by the document/information owner. In processing requests for public access to EFSA internal documents pursuant to the PAD Regulation, the assessment is based on the system of exceptions to reactive disclosure laid down in Article 4 of the PAD Regulation, including the existence of any overriding public interest in disclosure.

Unique identifier	A sequence of digits or letters, or both, unambiguously assigned to a record by a machine or person and which identifies that record as unique and distinct from all other records
Usability	A usable document is one that can be located, retrieved, presented and interpreted. It should be capable of subsequent presentation directly connected to the business activity or transaction that produced it.

Roles and responsibilities	EFSA's Management Accountable for the cascading of Information and Records Management objectives ensuring that the necessary requirements are monitored and integrated into EFSA's business processes. They are accountable for the compliance of their staff with this policy and responsible for nominating at least 1 Document Management Correspondent (DMC) and back-up to ensure that records within their remit are managed according to it. They ensure that information and information systems within their remit are managed according to this policy and any related rules, guidelines and procedures, including the implementation of information security measures deriving from risk assessments. Document Management Function (DMF) Provides advice and training to EFSA's Management and the DMC network who cascade to all staff on RM issues. The DMF runs the DMC network and drives the RM continuous improvement process. DMCs implement this policy's requirements in their Unit and support all staff in performing their obligations under this policy. The DMF has an advisory role in supporting staff to achieve compliance. Legal Affairs Services and Data Protection Officer (DPO) Supports EFSA and its staff by providing advice and clarification on legal matters, confidentiality and personal data protection. Information Security Officer (ISO) Nominated by ED Decision concerning the function of an Information Security Officer within EFSA (EFSA/HUCAP/DEC/017). Additional responsibilities recorded in Annex 2 of ADMACT_039_ED Decision_EFSA HSE and Security. Users All EFSA staff, including statutory staff and non-statutory workforce (including SNEs and trainees) and third parties (such as interims, consultants, external service providers, external experts and other EFSA stakeholders) having access to EFSA information and information systems and who must comply with this policy and any related rules, guidelines and procedures.

Any suspected or actual security weakness, threats, events or incidents to EFSA information and IT systems must be immediately reported.

Important rules on "How to protect EFSA sensitive information", including a clean desk and clear screen policies, and information on reporting information security issues, can be found in the EFSA Information Security Manual.

EFSA's IT function
Supports compliance with this policy across the organisation for information and documents that are stored and captured on EFSA's electronic systems.

More details regarding roles and responsibilities, together with other RM information, can be found in the relevant process charter, which is integrated in the EFSA Process Architecture.

EFSA's Record Management Systems (RMS)	The management of EFSA's records is ensured by using trustworthy electronic systems. They are designed to capture, register, maintain and retrieve records while ensuring their continued integrity with appropriate evidential characteristics. EFSA's Record Management Systems (RMS) must be able to manage the following RM processes: • creation of records (and their labelling as such); • storage of records; and • disposal of records in accordance with EFSA's retention schedule. It must also ensure record integrity, confidentiality and availability (3 pillars of information security). The main RMS to be used in EFSA is EFSA's DMS. Other RMS may be used as necessary, following approval of the DMF. The list of these approved RMS can be found in EFSA's "IT System Catalogue" (Annex 4).
Registration and filing	Document registration: Documents held in EFSA's Record Management Systems are automatically classed as records. Documents held in alternative tools including Outlook, Teams, SharePoint, OneDrive and OneNote, as well as relevant text messaging and instant messaging, require registration into the appropriate Record Management System of EFSA in case they meet the relevant requirements. **Documents shall be registered as records** if they contain important information which is ***not short-lived*** **or** if they ***may involve action or follow-up by EFSA*** or one of its Units/Departments[7]. Records shall: • contain minimum but clear information on their business context (e.g. metadata such as record type, date, title, author, security classification, or metadata standards as defined for EFSA's data sets); • be clearly linked to the business process they support; • be registered in their original format, as part of EFSA's commitment to reducing duplication (e.g. the electronic version of an email is the official record while a printed copy is only a convenience copy); • be saved in a format/medium that is compatible with standard office applications used at EFSA; • be filed in corporate record-keeping systems that are managed and monitored by their respective application managers; and • be grouped together with records that relate to the same business activity/transaction/ project.

---

[7] Commission Decision (EU) 2021/2121 on records management and archives, Article 7(1).

	Filing: To ensure that records can be easily identified and retrieved when required in an efficient and effective way, they shall: • be filed and stored using a harmonised approach within EFSA's RMS. A list of record-types and their location shall exist to ensure a better management of EFSA's information assets, and to support an effective search and retrieval (see Retention schedule below); • be identified by a universal unique identifier (UUID); and • be indexed and described by a combination of minimum metadata. **Records should be stored in the appropriate Record Management System no later than 4 months after creation.** It is the responsibility of Process Owners to ensure proper guidance to users on the creation and management of Records, including any RMS-specific guidance (in collaboration with the system owner of the RMS).
File plan	The purpose of EFSA's file plan is to facilitate targeted record searching, to manage records in groups of similar characteristics, and to ensure that the context of individual records is clear over time. In order to ensure consistency, EFSA's file plan will be centrally managed and maintained by the DMF to reflect the business processes of EFSA. Regular validation of Units' file plans and access models (then transcribed into the EFSA record file plan by the DMF) shall ensure compliance with the Information Security Policy and Data Protection rules.
Retention schedule	Records shall be kept in EFSA's RMS for as long as they are needed to serve EFSA's business, legal, administrative, Internal Control Framework and financial requirements, as long as they are needed for their research/historical value, and as long as they are required for evidential purposes, in accordance with the established Retention Schedule (Annex 1). In accordance with Regulation (EEC, Euratom) No 354/83, amended by Council Regulation (EU) No 2015/496, EFSA shall also start pre-establishing its historical archives after 15 years in view of opening it to the public after the expiry of a period of 30 years starting from the creation date of the document in question (Council Regulation No 1700/2003). Records lifecycle: • The retention schedule for all EFSA records will be assigned based on the nature of the document. EFSA's Retention Schedule will identify all records to be kept and determine their lifecycle, including those

	containing personal data in alignment with the DPO as needed. • When a document becomes a record it is saved in the RMS, where the identified retention schedule will be applied and its retention period initiates. • When records reach the end of their retention period they shall either be deleted or become historical archives, where they will be declassified and made public after 30 years, subject to a final verification on any exceptions that still may apply. All other information (in the form of a document, a collection of data or in any other digital or analogue form) shall be disposed of as soon as the owner decides it is no longer needed. This information may be stored in collaborative working platforms for developing and maintaining a knowledge base supporting operational needs.
Historical Archives	Some records will be kept permanently as part of EFSA's Historical Archives. It is expected that only a low percentage of the records created and received in an organisation merit permanent preservation. These are records that: • Are created by and are therefore unique to EFSA. • Provide evidence of, or measure the impact of, EFSA's programs and activities. • Document the origins of EFSA, its legal status, rights and entitlements. • Provide evidence of the organisation and structure of EFSA. • Are generated by significant programmes, projects, events and activities. • Comprise regulations and procedures governing EFSA together with policies, deliberations, decisions and actions. • Document the mission and goals of EFSA and its success in meeting them. • Provide evidence of the efforts and influence of EFSA in implementing its mission and meeting its goals with respect to working with European bodies and institutions, the international community and other partners. • Do not duplicate information contained in other sets of records: information-rich summary records should be selected over bulky and routine data (e.g. annual financial statements rather than invoices, receipts and other financial information). • Comprise significant publications of EFSA. • Provide significant context and background to the archives (e.g. organigrams, historical narratives, selected press cuttings). To reduce the risk of destroying records that, with the benefit of hindsight, should have been retained, certain series of records that relate to the core business of the EFSA and have currently been identified for retention for a long period (15 or 20 years), but not identified as having potential historical value,

	will be re-appraised before the expiry of the retention period to decide whether, with a longer historical perspective, they should form part of the Historical Archives.
Information Security	EFSA shall ensure the confidentiality, integrity and availability of information by appropriate security measures based on information security risk assessment. While this evidently applies to information classified as Sensitive from the confidentiality point of view, even public information may need to be protected to preserve integrity and availability.
Security categorisation	Records and documents shall comply with security principles, and the rules related to personal data protection. Records and documents shall be categorised as **sensitive non-classified (for short: SENSITIVE)** if they fall in the definition above and need to be protected as such[8]. The author of a sensitive document is responsible for compliance with the information security rules including marking the document as sensitive. Content created by 3rd parties outside EFSA retains its original categorisation and shall be treated by EFSA with an equivalent level of categorisation unless the author agrees with a downgrading of the categorisation level. The Information Security Officer can give guidance on the appropriate EFSA categorisation level to be followed. Reference is made to Article 9 of the PAD Regulation which provides for the treatment of sensitive documents. Access to documents and records and the disclosure of information contained therein shall be compliant with the PAD Regulation and the Data Protection Regulation.
Preservation and Disposal	Depending on the record's format, further measures shall be developed and applied in order to guarantee the long-term (i.e. more than 15 years) or permanent preservation of records with long term or permanent value. Likewise, hard copy records must be stored in a controlled environment with adequate temperature, humidity and fire control systems in place. Procedures for the preservation of electronic records must take account of the obsolescence of RMS hardware, software, file format and media formats used for storage of electronic records and provide for alternate hardware, software, file format and media formats to which the records can be migrated. These systems also need to guarantee the adequate preservation of records' context and structure over time.

---

[8] See the Information Security Manual for rules on the protection of sensitive documents and mandatory markings, and Annex 2 of this policy for more details on the implementation of the key need-to-know concept.

	The responsibility for identifying systems that may soon become outdated rests with the relevant system's application manager.
Original (paper) documents	Standard practice is for original (paper) documents to be destroyed once they have been scanned into EFSA's electronic systems. Exceptions to this are documented in Annex 3.
Monitoring and review of the Information Management Process	In order to ensure the effectiveness of the Information Management Process, the process will be monitored regularly to ensure its continuing suitability, adequacy, effectiveness and alignment with evolving regulations and standards and EFSA's strategic direction.

ANNEXES

Annex 1 – EFSA's retention schedule

Annex 2 – Note re "need to know" principle

Annex 3 – List of documents for which an original (paper) copy should be retained for the duration of the retention period

Annex 4 - IT System Catalogue