ASIC
Australian Securities & Investments Commission

Information and records management policy

05/05/2023

About this policy

This document sets out the policy obligations required by all ASIC team members to capture, manage, store, preserve and deliver information and content related to organisational processes, wherever that information and content exists.

Contents

A Policy objective

Purpose

1 This policy supports ASIC team members (**we**, **our**, **us**) to create, store, access and use information to support ASIC's business requirements and ensure compliance with Australian Government policies, information management standards and legislation, including the *Archives Act 1983* (**Archives Act**).

2 This policy reinforces:

- the use of digital information and records management practices that comply with the Australian Government's *Building trust in the public record* policy, issued in January 2021
- strategic objectives in the Data and Information Governance Framework, to ensure we create, store and manage data and information in digital formats, and that information is complete, available and usable by those who need it for as long as they need it
- the One ASIC Principles, including the Share Everything You Can (SEYC) Principle.

For further information, email records.management@asic.gov.au.

Scope

3 This policy applies to:

- ASIC team members; Commission members and **Senior Executives** (including Executive Directors and Senior Executive Leaders); the Companies Auditors Disciplinary Board; and Australian Taxation Office (**ATO**) Registry employees working on ASIC systems; with all parties being collectively referred to as '**team members**', '**you**' or '**your**'.
- all information assets (records, information and data) in any format, created or received to support our business activities.

4 ASIC's SEYC Principle will not extend to ATO employees delegated to perform Registry functions who have access to ASIC systems and records.

B Information and records management

5 ASIC's records are a vital corporate asset that:

- provide evidence of our actions and decisions
- support policy formation, high-level decision making, business continuity, efficiency and productivity in program delivery, management and administration
- protect the interests of ASIC, our team members, clients and the community
- help ASIC deliver its services in consistent and equitable ways
- can be used and re-used to drive business efficiencies by harnessing precedents and organisational experience.

6 We are committed to meeting our responsibilities under the Archives Act, and implementing the Australian Government's information management standards, policies and best practice in our information and records management practices and systems.

7 We are committed to consolidating our digital information and records management practices to ensure:

- the majority of our records are created, stored and managed digitally
- the digital information is authentic, complete, reliable, accessible and useable for those who need it
- authorised business information and recordkeeping systems are in place and maintained so digital information can be relied upon as evidence and to ensure it is protected and preserved for as long as it is required
- we develop a culture that values effective digital information and records management practices.

Governing principles

Records must be accurate, reliable, complete and useable

8 ASIC business operations and activities rely on quality information that is accurate, reliable, complete and usable.

9 All team members have a responsibility to create and adequately describe full, reliable and verifiable information and records in the course of their work, including:

- communications made or received
- actions undertaken or observed
- research and investigations
- deliberations and decisions.

10 All team members must ensure that the appropriate descriptive metadata and security classifications are applied to or embedded in all information and records.

Records must be in a digital format

11 All information and records resulting from team members conducting business must be retained in a digital format in accordance with National Archives of Australia (**NAA**) regulations.

12 Incoming physical records should be scanned to appropriate digitisation standards and managed digitally.

13 Records created in a digital format ('born digital') are to be captured, stored, used and managed digitally within the corporate recordkeeping system or other authorised business information system as appropriate.

14 Business processes and practices should be carried out digitally using digital forms, digital authorisations and digital workflows, wherever possible.[1]

15 Digitised, converted or migrated records must be considered functionally equivalent to the source records for business, legal and archival purposes to ensure these records have the same degree of authenticity, integrity, reliability and usability as the source or original records.

Information is stored in the corporate recordkeeping system or authorised business systems

16 Our corporate recordkeeping systems are those that have been assessed as being appropriate for:

- managing the creation, capture and storage of records
- protecting the integrity and authenticity of records
- securing and providing access to records
- recording disposal of our records.

[1] The *Electronic Transactions Act 1999* allows for and acknowledges the validity of electronic documents, including digital signatures, unless specifically excluded by other Commonwealth legislation.

17 Where records are not captured in corporate recordkeeping systems, they must be captured and maintained within authorised business information systems.

18 All business information systems must meet minimum metadata standards and be evaluated against the NAA business systems assessment framework to ensure they meet functional requirements for information management.

19 Business units recommending the implementation of new business systems must demonstrate compliance with the functional requirements for information management through the Technical Design Authority.

20 Where a business information system is assessed as having failed to fully meet the functional requirements but is still authorised by the Digital Governance Sub-committee, the system owner is responsible for monitoring and controlling the risks of not complying with recordkeeping legislation and government policy.

Information is accessible and shared as appropriate

21 ASIC information must be stored in accordance with the SEYC Principle, which is intended to limit the practical impediments to sharing information.

22 Information should be restricted only when an exemption to the SEYC Principle applies or by approval of the relevant Senior Executive.

23 Team members should exercise their judgement and determine whether they have a genuine business reason for accessing information. In effect this means that without access to that information, they would not be able to properly or efficiently carry out their official ASIC duties while managing any potential conflicts of interest.

24 Inappropriate access to shared high-risk data is monitored through regular reporting. Any unauthorised access is reported to the business owner, and Security Services, Privacy and/or other relevant teams.

Transfer, retain and destroy information appropriately

25 Under the Archives Act, agencies are required to transfer any records of archival value to the NAA within 15 years of their creation if they are no longer being actively used, to ensure their preservation.

26 Records, data and information from our systems, and physical records, can only be destroyed by following authorised disposal processes issued by the Information Resource Centre.

Non-compliance

27 Our Code of Conduct requires all team members to comply with the law and our policies and procedures. If a team member has failed to comply with an obligation under this policy, they may be subject to disciplinary action under the Code of Conduct, up to and including termination of employment.

28 If you identify non-compliance with this policy, you must notify ASIC as soon as practicable, in accordance with the ASIC Code of Conduct (sharepoint.com).

29 Email records.management@asic.gov.au if you identify non-compliance with this policy. You may also report the breach to the People and Development team via their People Partner, Senior Executive Leader or Executive Director, or in writing via our SpeakUp program.

C Accountabilities and responsibilities

Accountability	Responsibilities
Commission	• Approve this policy following endorsement by the Digital Governance Sub-committee. • Provide sufficient support and resources to ensure the policy's requirements are successfully implemented. • Promote compliance with this policy and associated business rules and procedures.
Chief Information Officer	• Ensure ASIC's digital information and records management meets the obligations outlined in the NAA's *Building trust in the public record* policy and Archives Act requirements as they relate to the Chief Information Governance Officer role.
Chief Data and Analytics Officer	• Consider expectations for team members to meet information and records management obligations as part of master data management and governance.
Digital Governance Sub-committee	• Fulfils the NAA's requirement for an Information Governance Committee. • Oversee ASIC's digital information and records management obligations under the NAA's *Building trust in the public record* policy.
Team members and Commissioner members	• Comply with this policy and associated business rules and procedures. • Provide and/or seek advice on information and records management requirements that are unclear or require revision.
Senior Manager, Information Resource Centre	• Develop strategies to implement this policy. • Ensure digital information and records management practices, and procedures that support this policy, comply with ASIC's obligations and responsibilities as a Commonwealth agency. • Endorse a business information system as meeting the principles and records requirements in accordance with ISO 15489-1, Information and documentation – Records management, Part 1: Concepts and principles. • Oversee the recordkeeping functionality of all authorised business information and corporate recordkeeping systems. • Ensure all team members are aware of this policy's requirements. • Establish ASIC as a site of best practice for digital information and records management. • Monitor compliance with this policy.

Key terms

The definitions in AS ISO 15489 Records management and the *Archives Act 1983* apply to this policy, as well as the key terms defined here.

Term	Meaning in this document
All team members	Includes all Commission members, ASIC team members (permanent and temporary), members of the Companies Auditors Disciplinary Board, the Australian Tax Office Registry, secondees, consultants and contractors.
Business information systems	Systems that create, keep and manage digital records and metadata (information about records), or manage metadata while the records are held elsewhere. Examples include finance, personnel, workflow, case management and ministerial correspondence systems.
Commission member	A person appointed by the Governor-General as the Chairperson, the Deputy Chairperson or a member of ASIC under sections 9(2) and 10 of the *Australian Securities and Investments Commission Act 2001*.
Content owner	The Senior Executive or delegate who is the custodian of the information or records managed with a container. This is separate from the business owner. For example, the business owner may be responsible for the system as a whole while the content owner may be responsible for specific sections, forms or sites within the system.
Corporate recordkeeping system	An automated system used to manage the creation, use, maintenance and disposal of electronic and physical records, documents and content for the purposes of providing evidence of business activities. Such a system maintains appropriate contextual information (metadata) and links between records, documents and content to support their value as evidence.
Data	Facts and statistics presented in a structured or unstructured manner, and which are suitable for transmission, interpretation, or manual or automatic analysis.
Destruction	The process of eliminating or deleting records beyond any possible reconstruction.
Digital records	Records created, communicated and maintained by means of computer technology. They may be 'born digital' (that is, created using computer technology) or they may have been converted from their original format into a digital format (for example, scans of paper documents).[2]

[2] National Archives of Australia – Digital Records

Term	Meaning in this document
Disposal	A range of processes associated with implementing appraisal decisions that include the: • retention, deletion or destruction of records • migration or transmission of records • transfer of custody or ownership of records.
Enterprise content management	The strategies, methods and tools used to capture, manage, store, preserve and deliver content and documents related to organisational processes. These strategies, methods and tools enable management of an organisation's unstructured information, wherever that information exists.
Evidence	Material that can be introduced into court proceedings to prove the facts and issues alleged by the parties.
Functional equivalence	Copies or reproductions that have the same degree of authenticity, integrity, reliability and usability as the source or original records.
Information	Data about someone or something that is presented in context. Information is derived from data after it has been processed and presented in context—in this way, data is given meaning. Information is the result of gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.
Information asset	Includes records, information and data that are created, collected, received and kept as part of government business.
Information management	Methods for finding, using and sharing an agency's information assets to meet government and community needs. Good information management makes these processes easy and maximises the value of information.
Metadata	Structured, machine-processible information that describes and/or allows information to be found, managed, controlled, understood or preserved over time.[3]
Record[4]	Any item or information that has been created, sent and received while carrying out ASIC's business operations. Records provide proof of what happened, when it happened and who made the decisions. Not all records are of equal importance or need to be kept. Records have many formats, including paper, digital, email, data, sound and video-recording . Data and datasets retained in business systems are Commonwealth records and must be managed in accordance with the *Archives Act 1983*.

[3] Australian Government Locator Service Metadata Standard: Part 1, Version 2.0
[4] Adapted from the *Archives Act 1983*, Part I, Section 3; Standards Australia, AS ISO 15489, Part 1, Clause 3.15

Term	Meaning in this document
Recordkeeping[5]	Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information. Includes the creation of adequate records of business activities; the design, establishment and operation of accurate recordkeeping systems; and the management of records used in business (traditionally regarded as the domain of records management) and as archives (traditionally regarded as the domain of archives administration).
Records authority	An instrument issued by the National Archives of Australia to give its approval to Australian Government agencies or other organisations or persons to dispose of Commonwealth records.
Records management[6]	The efficient and systematic control of the creation, receipt, maintenance, use and disposal of records. Includes managing processes for capturing and maintaining evidence of and information about business activities and transactions, in the form of records.
Senior Executive	A Senior Executive Leader or Executive Director.

[5] Adapted from: Standards Australia, AS ISO 4390, Part 1, Clause 4.19; and Part 3, Foreword, NAA Glossary
[6] Adapted from: AS ISO 15489, Part 1, Clause 3.16

Supporting resources

ASIC supporting procedures

- Information and Records Management Procedures
- Records Disposal Procedures (*not yet available*)

ASIC supporting policy documents

- Data and Information Governance Framework
- Handling Sensitive and Classified Information Protocol
- Need to Know Guidelines
- Share Everything you Can Principle and Exemptions
- Security Policy

ASIC Key Information Systems

- SharePoint ECM
- CRM and RCR SharePoint
- Authorised business systems

Other related information

Information management legislation

- *Archives Act 1983*
- Archives Regulations *1983*
- *Senate Continuing Order for the production of departmental and agency file lists* (the 'Harradine Motion')

Commonwealth legislation that includes information management requirements

- *ASIC Act 2001*
- *Crimes Act 1914*
- *Electronic Transactions Act 1999*

- Electronic Transactions Regulations 2000
- *Evidence Act 1995*
- *Fair Work Act 2009 and Regulations*
- *Freedom of Information Act 1982*
- *Freedom of Information (Charges) Regulations* 2019
- Freedom of Information (Disclosure Log – Exempt Documents) Determination 2018
- *Privacy Act 1988*
- *Privacy Regulation* 2013
- Legally binding privacy guidelines and rules
- Protective Security Policy Framework
- *Public Governance, Performance and Accountability Act 2013*
- Commonwealth Procurement Rules
- *Public Service Act 1999*
- *Public Service Regulations 1999*
- *Australian Public Service Commissioner's Directions 2022*

Information management standards and policies

- *Building trust in the public record policy*, 2021 (National Archives of Australia)
- Information Management Standard for Australian Government
- Australian Government Recordkeeping Metadata Standard Version 2.2
- AGLS Metadata Standard (AS5044: 2010)
- ISO 16175-1:2020 Processes and functional requirements for software for managing record

Document control

Policy ownership

Information Resource Centre / Enterprise Services, SEL is responsible for the development and implementation of this policy.

This policy is reviewed in accordance with ASIC's Enterprise Policy Design and Review Handbook.

Policy approval

Version	Approver	Approval date
V1.0	Warren Day	22/10/2021
V1.1	Zak Hammer	5/05/2023

Version history

Version	Changes	Approval date
V1	Updated Information, Records and Knowledge Management Policy (issued 2017)	1/10/2021
V1.1	Updated Information and Records Management Policy to align with the Enterprise Policy Framework	5/05/2023
V1.2	Minor updates including links to relevant procedures and header	17/07/2023

Distribution

Version	Distribution list	Effective Date
V1	All teams	October 2021
V1	Digital Governance Sub-committee	11/10/2021
V1.1	Digital Governance Sub-committee	22/05/2023
V1.1	All teams	12/06/2023
V1.2	All teams	17/07/2023