FOI 189-2023 DOC 1

ASIC
Australian Securities & Investments Commission

Information and Records Management Procedure

11/08/2023 v2.0

About this document

This procedure supports 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

Information and Records Management Procedure 1

About this document 1

Contents 2

Document objective 3

Purpose 3

Scope 3

A Information and Records Management Procedure 4

1. Maintain accurate, reliable, complete and usable information and records 4
2. Records must be in a digital format 4
3. Information is stored in the corporate recordkeeping system or authorised business systems 5
4. Information is accessible and shared as appropriate. 6
5. Transfer, retain and destroy information appropriately 7

B Accountabilities and responsibilities 8

C Key legislation, policies and guidance 10

Table 1: Specific requirements to or referenced within this procedure

Document control 11

Document objective

Purpose

This procedure supports:

- all team members to comply with the governing principles set out in the *Information and Records Management Policy* and create, store, access, use and dispose of information in accordance with ASIC's business requirements and to ensure compliance with the Australian Government legislation, policies, and information management standards.
- For further information email records.management@asic.gov.au

Scope

This procedure 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.

A Information and Records Management Procedure

This section provides you with guidance to adhere to the **governing principles** set out in the Information and Records Management Policy:

1. Maintain accurate, reliable, complete and usable information and records

- As a Commonwealth agency, ASIC is bound and required to manage the information and records we create and hold for both legal and business reasons. This means that our records need to be available, accessible and protected from accidental or intentional deletion.
- A business-value record is 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.
- Specific examples of recordkeeping responsibilities for teams and team members are set out in Part B: Accountabilities and responsibilities.
- The Information Resource Centre provides guidance and training on creating, managing, and storing information and business value records.

2. Records must be in a digital format

- Most new ASIC's records are created and managed digitally by design. This includes records created:
  - by office applications – for example, word-processed documents, spreadsheets, presentations and desktop-published documents
  - in online and web-based environments such as intranets, internets and public websites
  - by business information systems such as databases, geospatial data systems, human resources systems, financial systems, workflow systems, client

management systems, and document and records management systems (like SharePoint)

- by digital communication systems such as email, SMS (short messaging services), MMS (multimedia messaging services), voicemail, social media, instant messaging, video conferencing and teleconferencing.

- There are instances where information and records are received, printed, stored and managed in a physical (paper) format.

- The scanning and destruction of original or source records must be carried out in accordance with the NAA's digitisation specifications, retention authorities and any associated ASIC policies, rules and procedures.

- The Information Resource Centre provides guidance on the efficient and appropriate use of digital and paper resources including digitisation standards.

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

- All teams members are required to save information and records created in the course of their work for ASIC in the corporate recordkeeping system or an authorised business system.

- ASIC's corporate recordkeeping systems are dedicated to ensuring the creation and maintenance of authentic, reliable, and usable records for as long as they are required to support business functions and activities.

- s 47E (d) [redacted]

- s 47E (d) [redacted]

- s 47E (d) [redacted]

- Data and datasets retained in business systems, like other information created and received in connection with ASIC's

business, are Commonwealth records and must be managed accordingly.

- s 47E (d) [redacted]
- s 47E (d) [redacted]
- The register of authorised business information and corporate recordkeeping systems will be maintained by the Information Resource Centre.

4. Information is accessible and shared as appropriate.

- s 47E (d) [redacted]
- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- [redacted]
  - [redacted]
  - [redacted]
- [redacted]

s.47E (d) [redacted]

5. Transfer, retain and destroy information appropriately

- Records should be routinely disposed of in accordance with:

  (a) Section 24 of the *Archives Act, 1983* and a current approved record authority;

  (b) normal administrative practice (NAP).

- All team members should follow the Records Disposal Procedure issued by the IRC, which includes guidance on sentencing, destruction, NAP, migration, disposal freezes and transfers.

- All processes automating or incorporating deletion or destruction activities must be discussed with IRC during development stages.

- Retention of records, data and information beyond the authorised disposal date increases the ongoing costs associated with managing digital and paper information and increases potential risk and liabilities for holding information which could have otherwise been legally destroyed. These need to be considered prior to any decision to retain information that is eligible for disposal.

- Back-scanning of older paper-based records should be carried out only where there is a specific and approved business case to do so and in accordance with the NAA's digitisation specifications, retention authorities and any associated ASIC policies, rules and procedure.

- Effective quality assurance controls are essential if digitised, converted, and/or migrated records are to stand in place of source records, where ASIC will rely on scanned copies as official versions for ongoing business.

B Accountabilities and responsibilities

Accountability	Responsibilities
Team members and Commissioner members	Comply with the Information and Records Management policy, associated business rules and procedures. Provide and/or seek advice on information and records management requirements that are unclear or require revision.
Decision makers for system procurement and implementation	Comply with all relevant standards, guidelines and policies on information and, records management with regard to the procurement and development of business information systems.
ICT team members, system administrators & business system owners	Ensure that recordkeeping and information management functionality is addressed for any information systems purchased, developed and implemented, including demonstrating how systems meet requirements set by National Archives of Australia; Assess systems for inclusion on the authorised business information and corporate recordkeeping systems register; and Maintain the technology used to support systems that capture and keep information and records digitally ensuring that all information is reliable, available and accessible to team members when required.
Information & Records Management team	Create and maintain business rules and procedures to support the Information and records management policy; Promulgate the Information and records management policy and associated business rules and procedures to all team members; Monitor compliance with the Information and records management policy and procedures; Deliver digital information and records management training and advice to all team members; and Maintain, monitor and review authorised business information and corporate recordkeeping systems under their control.
Senior Executives (Executive Directors and	Consider expectations to meet information and records management obligations during performance assessments.

Senior Executives Leaders)	Monitor team members under their supervision to ensure that they understand and comply with this policy and associated business rules and procedures; and Support and foster a culture within their workgroup that values and promotes effective digital information and records management practices.
Managers/Officers responsible for engaging and managing contracted service providers	Ensure that contracted service providers are aware of information and records requirements; and Include information and records requirements in contracts, including clarification of information ownership and intellectual property, and relevant matters concerning storage, privacy and confidentiality.
Boards, Working Parties and Project Teams (Chair or Project Manager)	Must be responsible for the management of board records; Comply with all relevant standards, guidelines and policies on information and records in regard to records of the board, working party or project team; Create and keep full and accurate records of all board, working party or project team meetings; and Register all meeting papers in an authorised business information system or the corporate recordkeeping system (including all agendas, agenda papers, minutes, draft reports, reports and decision pages).

C Key legislation, policies and guidance

The Information and record management policy and procedures supports and improves ASIC's ability to comply with requirements and obligations as set out in a broad range of legislation impacting recordkeeping. Table 1 identifies specific requirements to or referenced within the procedure.

Table 1: Specific requirements to or referenced within this procedure

Legislation/Policy	Description
Archives Act, 1983	The Act applies to all Commonwealth records and empowers the National Archives of Australia (NAA) to preserve the archival resources of the Australian Government. Under the Act, it is illegal to destroy Australian Government records without permission from the Archives unless destruction is specified in another piece of legislation or allowed under normal administrative practice (NAP). The Act also establishes a right of public access to non-exempt Commonwealth records.
Data and Information Governance Framework	ASIC's Data and Information Governance Framework is a conceptual structure and set of rules that outlines how data and information is managed and controlled across ASIC. It describes who can do what with data and information, under what circumstance, using what systems and methods and the associated accountabilities, both internally and externally.
Building trust in the public record 2021	This National Archives of Australia policy promotes a consistent approach to information governance across the Australian Government and within individual agencies. It applies to government information, data and records, as well as systems, services and processes, including those created or delivered by third parties on behalf of Australian Government agencies.
Electronic Transactions Act, 1999	This Act encourages online business by ensuring that electronic evidence of transactions is not invalidated because of its format. The act allows for and acknowledges the validity of electronic documents including digital signatures unless specifically excluded by other Commonwealth legislation.
Evidence Act, 1995	This Act provides for documents created and maintained in paper and electronic form to be admitted in evidence before federal courts.
Freedom of Information Act, 1982	The Act, which applies to Australian Government ministers and most agencies, provides a right of access to most government-held documents, other than exempt documents.
Privacy Act, 1988	All team members must take steps to protect personal information according to the *Privacy Act, 1988* and the Australian Privacy Principles.
Protective Security Policy Framework	The PSPF sets out government protective security policy and supports entities to effectively implement the policy across the following outcomes: security governance, information security, personnel security, physical security.

Document control

Document ownership

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

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

Document approval

Version	Approver	Approval date
1.0	Zak Hammer, ED Operations	05/05/2023
2.0	Diana Steicke, SEL, Intelligence & International	11/08/2023

Version history

Version	Changes	Approval date
1.0	First issue	05/05/2023
2.0	Extended guidance on all record formats 1.0, 2.0, updates to roles and positions	11/08/2023

Distribution

Version	Distribution list	Effective Date
1.0	Digital Governance Sub-committee	22/05/2023
1.0	All team members	12/06/2023
2.0	All team members	15/08/2023