Disposal Standard

Version: 1.0

Date Finalised: 01/09/2021

Date for Review: 01/09/2024

STATE RECORDS
of South Australia

Government of South Australia
State Records

Disposal Standard

The Standard

Authority

This Disposal Standard (Standard) is issued under section 14(1) of the *State Records Act 1997* (SR Act).

Agencies must dispose of their information assets in accordance with the requirements set out in the SR Act and this Standard.

Scope

This Standard applies to all government agencies, and the information assets of those agencies, as defined in section 3(1) of the SR Act.

In this Standard, the term 'information asset' should be taken to incorporate the definition of official record as defined by section 3(1) of the SR Act.

The term 'information asset' refers to information, data and records, in any format (whether digital or hardcopy), where it is created or received through the conduct of government business.

Executive Summary

The Standard provides a set of mandatory principles and requirements for South Australian government agencies regarding the disposal of government information.

Implementation of this Standard enables the disposal of information assets to be carried out lawfully and efficiently and ensures the permanent retention of information of importance to the State. This benefits efficient business operations, reduces costs and supports compliance with regulatory requirements such as the SR Act, the *Freedom of Information Act 1991*, and the *Information Privacy Principles Instruction* (PC012). This Standard also supports the principles in the Information Management Standard.

Disposal

Introduction

State Government agencies and local government authorities must only dispose of information assets in accordance with a determination made by the Director of State Records with the approval of State Records Council.

A determination provides authorisation for information assets to be destroyed or transferred to non-government entities and comes in the form of either a disposal schedule or a transfer of ownership and custody schedule.

Disposal is 'a range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments' (AS ISO 15489).

Disposal includes:

- Destroying information assets
- Abandoning information assets
- Migrating information assets from one system or platform to another
- Transferring ownership or possession of information assets (not including transfer to State Records, or to another government agency)
- Selling information assets.

Information assets, including emails, social media posts and data in business systems, cannot be destroyed, or given to non-government entities outside of State or Local Government without this authorisation.

In addition, information assets must not be abandoned, sold, nor damaged or altered without authority.

Disposal principles

Five principles guide the disposal of information assets:

1. Disposal is authorised
2. Disposal is underpinned by appraisal
3. Disposal is managed
4. Disposal is complete and secure
5. Disposal is accountable.

Disposal requirements

Each principle is underpinned by a set of requirements that agencies are expected to meet.

Guidelines associated with this Standard will assist agencies to implement the requirements of this Standard.

Principle 1: Disposal is authorised

Disposal of the agency's information assets is undertaken in a lawful manner.

Requirements

Principal officer must:

- ensure that disposal of information assets is conducted in accordance with the SR Act and standards issued under the Act.

Agencies must:

- only dispose of information when no longer required for business or legal purposes, and in accordance with current disposal schedules issued by State Records and approved by State Records Council.
- ensure that no information assets are disposed of unless in accordance with current, approved disposal schedules.
- not sell, abandon, or donate information assets to non-government entities.
- seek a disposal determination for operational information assets not covered by current, approved disposal schedules.
- authorise internal policies and procedures for disposal of information assets in accordance with the SR Act.
- ensure that either the agency heads or delegated officers signs off on the destruction of information assets and ensure the disposal process is documented.

Principle 2: Disposal is underpinned by appraisal

Disposal decisions are derived from an appraisal process to ensure all business information assets are covered and disposal decisions are accountable.

Requirements

Agencies must:

- identify, analyse and document requirements for retaining legacy, current and future information assets based on business and legal context, including knowledge of business functions, activities and processes and specific legislation and regulation.
- undertake appraisal in accordance with State Records' standards, including providing rationale for permanent retention of information assets in accordance with appraisal standards.
- ensure appraisal covers all legacy information assets in their control including physical and digital formats regardless of locations and/or systems.
- consult relevant internal and external stakeholders when undertaking appraisal.
- review appraisal decisions, including those decisions in approved records disposal schedules, when there are significant business, legal or machinery of government changes.

Principle 3: Disposal is managed

A disposal program is an integrated part of the agency's overall program for managing its information assets, to enable the disposal of government information to be carried out in a planned and accountable way. This ensures business needs and legislative obligations are met, and risks are minimised.

Requirements

Agencies must:

- develop and implement a disposal program in accordance with this Standard.
- develop and implement disposal policies and procedures to ensure staff and contractors understand their obligations under the SR Act.
- ensure staff and contractors are aware of their responsibilities for the retention and disposal of information assets.
- ensure specialist staff or contractors are appropriately skilled and have the capability to undertake disposal tasks.
- ensure disposal schedules, including transfer of custody schedules, are used correctly and appropriately.
- ensure information assets remain accessible in a readable form until legally disposed of. (Note: where information assets are not able to be accessed, this is considered a form of disposal).
- migrate digital information assets as systems, software and media are upgraded or become obsolete to ensure information assets remain accessible for as long as they are required.
- only destroy information assets when no longer required for business or legal purposes, and in accordance with current, approved records disposal schedules issued by State Records.
- must dispose of information assets in a timely manner once all business, legal and accountability requirements have been met.
- design or implement information systems according to relevant standards to support the effective disposal of information assets.
- retain information assets within their control and / or custody at all times, ensuring information assets do not get abandoned, lost, given away or taken out of the agency without authorisation.
- ensure disposal plans, programs, policies and procedures are monitored regularly to ensure they remain current and effective.
- ensure hardcopy source information assets are disposed of legally following digitisation in accordance with GDS 21.
- ensure any information assets held by non-government entities are returned, where required, to the agency for destruction or transfer to State Records.

Principle 4: Disposal is complete and secure

The destruction of government information assets (including hardcopy, digital and hybrid) is undertaken using complete, irreversible and secure methods to ensure the content and related metadata are not released.

Migration or transfer of information assets from their original context is done in a way to ensure their ongoing authenticity, reliability, integrity and usability.

Requirements

Agencies must:

- ensure methods used to destroy information assets are complete and irreversible, including methods applied to digital information assets, e.g. shredding or pulping for hardcopy information; reformatting, rewriting or erasure for digital information.
- ensure environmentally sound methods of destruction are used where possible.
- ensure destruction of sensitive or confidential information assets is undertaken using secure processes that ensure that information remains protected at all times.
- ensure destruction of information assets actually occurs whether undertaken in-house or by a third party provider.
- ensure exact duplicate copies of information assets are destroyed at the same time, or shortly after, the originals, where appropriate.
- ensure data required to be retained is migrated, so that its integrity is maintained, and it remains accessible, or else is retained in the original system until able to be disposed of legally.
- ensure information assets are securely transferred to non-government entities, where this is authorised under disposal determinations.
- ensure all permanent information assets from the same records system are securely transferred to State Records, where the transfer is approved in accordance with the *Transfer of Official Records Standard*.

Principle 5: Disposal is accountable

The agency is able to provide evidence of when and why any form of disposal of information assets has occurred to demonstrate compliance with the SR Act, the PC012 and disposal determinations.

Requirements

Agencies must:

- maintain documentation of all information assets held, including evidence of all information assets disposed of by destruction or transfer.
- document the research, analysis and assessment of requirements underpinning disposal decisions and actions.
- retain proof of the relevant disposal schedule or determination, date of disposal, and internal authorisation for all information assets destroyed or transferred.

Management of risk

There are risks associated with disposal processes which require monitoring and potential action. Causes and sources of risks include:

- environmental hazards (e.g. flood, fire) resulting in permanent damage or loss of information assets
- ICT infrastructure failure or compromise (e.g. hacking, viruses) that delete or corrupt digital information assets
- use of legacy or bespoke software that is not capable of enabling comprehensive or accurate migration of data to a replacement system
- information that is inaccessible because it is stored on media that is damaged or obsolete, e.g.:
    - degraded magnetic media
    - media for which there is no longer hardware available, or
    - where software is no longer usable.
- staff practices not meeting agency policies and procedures for the disposal of information assets, e.g.
    - destruction of information due to deliberate action, accidental action, or lack of knowledge
    - lack of accountability trails for disposal decisions
    - incomplete destruction resulting in remaining information assets being accessible and / or discoverable
    - taking information assets offsite or donating them to non-government entities.

Application of this Standard and other State Records standards and guidelines will reduce or avoid those risks.

Date approved	Approved by	Date for review	Version
01/09/2021	Attorney-General	01/09/2024	Final 1.0

Need further assistance?

State Records
Tel (+61 8) 8204 8791
Email staterecords@sa.gov.au
Web www.archives.sa.gov.au