Information Management Standard

Information Management Standard

Introduction

The appropriate management and control of information and data is crucial for the effective delivery of government functions and services. Good information and data management practices are the basis of good government; supporting evidence-based decision making, the development of policy, joined-up service delivery and accountability.

Effective management of information and data supports innovation and the transformation of service delivery, enabling communities and individuals from across South Australia to transact with government and stay informed of government decisions.

Purpose

The Information Management Standard establishes the principles and behaviours expected of agencies in managing government information and data (referred to as *information*) to achieve their own business objectives and to meet requirements under their legislative and policy obligations.

The Standard is consistent with the concepts of International Standard ISO15489 (2017).

Authority

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

State Government agencies must manage their information assets in accordance with the requirements set out in this standard.

Definition

For the purposes of this Standard *information assets* refer to information, data and records, in any format, where it is created or received through the conduct of government business.

Principles

The management of government information is based on five principles:

1. The value of information is known
2. Information is created and managed appropriate to risk
3. Ownership of information is assigned
4. Information can be relied upon
5. Information is available as required

Behaviours

Each principle is underpinned by a set of behaviours that agencies must demonstrate in order to ensure their information management practices align with government expectations.

A series of tools have also been identified that are, or will be available, to support agencies in achieving these behaviours.

Principle 1: The value of information is known

Information is treated as an asset of the agency; its value, both current and future, is determined, understood and leveraged to improve business outcomes.

Behaviours

» Agencies identify and document what their information assets are, where they are stored and who is responsible for their management;

» Agencies understand and document how their information assets support their business objectives and operations or their compliance obligations;

» Agencies must ensure information assets are linked to business functions and objectives;

» Agencies induct and train staff in their information management responsibilities; and

» Agencies foster an organisational culture that values and manages information as an asset and an enabler for business.

Principle 2: Information is created and managed appropriate to risk

Agencies understand what information needs to be created and kept to support business objectives, meet compliance obligations and mitigate risk.

Behaviours

- » Agencies analyse and document what information must be created and managed across the organisation applicable to the regulatory environment in which they operate;

- » Agencies develop and issue policies outlining how information will be managed in their organisation;

- » Agencies assess the business risks of not creating or managing information where there is a legal or evidential need;

- » Agencies manage information digitally unless there are specific legal reasons for keeping physical records;

- » Agencies design and implement information systems according to relevant standards so that they support the effective management, identification and disposal of information;

- » Agencies store information appropriately, to ensure it remains accessible for as long as required;

- » Agencies only destroy information when no longer required for business or legal purposes, and in accordance with current, approved records disposal schedules issued by State Records; and

- » Agencies review and audit how well their information management policies and practices support their business.

Principle 3: Ownership of information is assigned

Responsibility for the governance of information is assigned appropriately in order to ensure information is managed for the best outcomes of the agency, its customers and broader community.

Behaviours

- » Agencies assign internal responsibility for information assets to business owners;

- » Agencies ensure that assigned owners are aware of their responsibilities in managing the information assets assigned to them;

- » Agencies ensure responsibilities for information management are delegated appropriately, in writing;

- » Agencies ensure that roles and responsibilities relating to the management of information assets are defined in policy or other internal documents;

- » Agencies ensure that ownership and accountability for information is managed consistently through a governance structure; and

- » Agencies monitor and report on staff adherence to internal information management policies.

Principle 4: Information can be relied upon

Policies, practices and systems are implemented that ensure information can be relied upon as trusted and authentic evidence of decisions made and actions taken.

Behaviours

- » Agencies make and keep full and accurate records of business activity, appropriate to their business processes, regulatory environment and risk and accountability requirements;

- » Agencies ensure information is saved into organisational systems that meet relevant standards in a timely manner, ensuring information is reliable, authentic and trusted;

- » Agencies record relevant details (metadata) in systems so that the business context of information can be readily understood e.g. the type of business transaction, when it occurred, who was involved, etc.;

- » Agencies use established and existing definitions of information where possible, so that there is consistency in how entities are identified and reported on across Government; and

- » Agencies implement practices and systems so that the quality and authenticity of information is assured.

Principle 5: Information is available as required

Information is accessible for as long as needed and is shared appropriately (subject to access, security, and privacy rules) within a protected and trusted environment.

Behaviours

» Agencies implement information security classifications and requirements that are applicable to the sensitivity of the information;

» Agencies remove access restrictions on information as soon as they no longer apply, once sensitivity has diminished;

» Agencies migrate digital information as systems, software and media are upgraded or become obsolete to ensure it remains accessible for as long as it is required;

» Agencies identify requirements for retaining operational information not covered by general disposal schedules, and seek a disposal determination for these records in the form of a records disposal schedule;

» Agencies ensure that no information of corporate value is destroyed unless in accordance with current, approved disposal schedules;

» Agencies collect and manage personal information in accordance with privacy principles;

» Agencies share information across government unless legally prohibited or restricted by some other means;

» Agencies proactively publish information in line with government policy; and

» Agencies do not sell, abandon or donate government information to external parties where such action would result in the agency not having access to that information or without authorisation.

Resourcing

Sufficient allocation of resources, including budget, infrastructure and staff, is a vital component of an agency's information management program. Staff allocated to perform information management related functions must be appropriately skilled and have the capability to manage their agencies information management assets in accordance with this Standard.

Planning

Like any organisational asset it is important that the management of an agencies information is considered and planned at an enterprise-wide level. An information management plan is a core elements of an agency's information management program and should be developed to support the agency's broader strategic and corporate goals and objectives.

The information management plan, which should be supported by a broader governance model incorporating policies, procedures, education and technology, provides high-level direction and must be consistent with legislative and business requirements.

Progress against the plan should be regularly assessed and reported on.

Governance Model

The management of an agencies information assets should occur in a governance model that includes:

- Policy and Procedure
- Defined Resources, Roles and Responsibilities
- Access and Discovery Schemes
- Education
- Compliant Systems
- Information Management Plan
- Information Asset Audit
- Self-Assessment and Reporting
- Security and Privacy Protection
- Disposal Determinations
- Risk and Value Assessment

Information Management Program

Date approved	Approved by	Date for review	Version
18 June 2019	Attorney-General, SA	31 Dec 2021	1.1

Need further assistance?

State Records

Tel (+61 8) 8204 8791

Email staterecords@sa.gov.au

Web www.archives.sa.gov.au