

# Standard

## Contracting and Information Assets

Version: 1.3

Date Finalised: 21/04/2023

Date for Review: 30/06/2024

**STATE RECORDS**  
of South Australia



Government of South Australia  
State Records

# Contracting and Information Assets Standard

## The Standard

### Authority

This Contracting and Information Assets Standard (Standard) is issued under section 14(1) of the *State Records Act 1997* (SR Act).

Further, section 13 of the SR Act states that every agency must ensure that information assets in its custody and legal possession are maintained in good order and condition.

Agencies must ensure that any contracting arrangements they enter into with contracted service providers include information management practices that comply with the SR Act, *Freedom of Information Act 1991* (FOI Act), the Premier and Cabinet Circular 012 – Information Privacy Principles Instruction (IPPI) 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.

The term ‘contracted service provider’ refers to a non-government party that has either entered into an agreement with an agency to provide goods or services required by the agency to meet business activities and functions, or information management functions and responsibilities to the agency. While the contracted service provider may be an independent business entity that takes responsibility for risks, the management of information assets created, kept and used under agreement are often treated as if managed by the agency.

This Standard must be read in conjunction with the following Standards:

- » Information Management
- » Managing Digital Records in Systems
- » Minimum Recordkeeping Metadata Requirements
- » Disposal.

### Executive summary

The Standard provides a set of mandatory principles and requirements for agencies regarding the contracting out of government information assets and information management responsibilities to contracted service providers. It also supports the principles in the Information Management Standard.

Agencies must apply the Standard in all cases where an agency is planning to enter into a contract where a service is to be undertaken on behalf of the agency and ownership and legal possession (legal right of access) of the information assets

associated with the service remain with the agency. This includes services that were previously considered core functions of an agency, for example case management. There may be instances where its application is limited or unnecessary.

This Standard:

- » does not constitute legal advice. Agencies should seek legal advice when entering into contractual arrangements
- » is not intended for use in cases of sale or privatisation of agency enterprises or activities. It also excludes grant-funding relationships and occasions where agencies resume full operational responsibility for a previously outsourced activity.

## **Contracting out of information assets management responsibilities**

To ensure that the accountability and efficiency of agency and government administration is not diminished as a result of contracting, agencies must ensure that contracting arrangements include information management practices that meet the government's legislative obligations and requirements. Of particular importance are information assets that contain the personal affairs of any person.

Legal possession (and therefore ownership) of the information assets of the contracted business activity remains with an agency regardless of the custody arrangements.

Where an agency's business activity is conducted by contracted service providers the agency's information management obligations extend to those contracted service providers.

Therefore, agencies have an obligation to define information management responsibilities of contracted service providers.

## **Contracting Principles**

The following principles must be followed during the contracting process with contracted service providers:

1. Risks to information assets are identified and addressed
2. Ownership and custody of information assets are defined
3. Creation and control requirements are specified
4. Disposal processes of contracted information assets are specified
5. Access to information assets is guaranteed
6. Storage requirements are specified
7. Security measures are specified
8. Monitoring and auditing processes are established/specified
9. Post completion information management obligations and requirements are specified

## Behaviours

### Principle 1: Risks to information assets are identified and addressed

A risk assessment must be undertaken with specific consideration given to the complexity of the contract and sensitivity of the information assets to determine what information management requirements need to be included in the contract.

#### Behaviours

Agencies must:

- » undertake a risk assessment with specific consideration given to the complexity of the contract and the sensitivity of the information, this includes any privacy risks
- » document all risks identified as part of their risk management program
- » consult with all relevant bodies or parties, including but not limited to:
  - the agency's:
    - Records Manager
    - Privacy Officer
    - Accredited FOI Officer
  - the Crown Solicitor's Office (or other appropriate legal counsel) and
  - the agency's accredited purchasing unit and contract management staff

to discover any documents and / or agency experience that would assist them in drafting the tender and contract documentation

- » ensure that procedures are in place to handle issues relating to contracts where information may traverse jurisdictional borders. This may be a factor when contracting with offshore subsidiary companies and offshore parent companies. (In some jurisdictions there is a requirement for special considerations for trans-border data flow of personal information).

### Principle 2: Ownership and custody of information assets are defined

Identification of information asset ownership, legal possession and custody arrangements must be established in the contract.

#### Behaviours

Agencies must:

- » ensure the contract specifically identifies ownership and custody arrangements for the following information assets:
  - relating to the contracted service that remain the property of the agency, including information assets created during the contract
  - where ownership will be transferred to the contracted service provider and when this will happen
  - created by the contracted service provider as a result of the service provided under the contract which will become information assets and therefore the property of the agency
- » ensure transfer of ownership of information assets (from agency to contracted service provider or from contracted service provider to agency), is done via a current Transfer of Ownership and Custody Schedule (TOCS) approved by the State Records Council

- » consider ensuring that the contract specifies ownership of intellectual property in the information assets, including existing information assets and those created during the term of the contract
- » consider (as much as possible) the risks associated with transferring physical possession of permanent value information assets to a contracted service provider. Where information assets of permanent value are in the physical possession of the contracted service provider the agency must apply any conditions necessary to ensure their protection and their safe return to the agency.

### **Principle 3: Creation and control requirements are specified**

All information assets to be created, or captured, under the contract must be documented in the contract and managed appropriate to risk and in accordance with the SR Act, to ensure they can be relied upon and trusted as authentic evidence of decisions made and actions taken.

#### **Behaviours**

Agencies must:

- » identify in the contract any legal requirements to create information assets
- » identify in the contract those information assets that need to be created to ensure continuity of business and ensure its accountability and statutory obligations are met
- » ensure that the contracted service provider establishes control systems for all agency-owned information assets before any information assets are transferred to the contracted service provider
- » ensure, via the contract, that any information assets created, generated or received by the contracted service provider are managed and stored in a compliant system in accordance with the Managing Digital Record in System Standard and the Minimum Recordkeeping Metadata Standard.

Further information on compliant systems can be found in the Managing Digital Records in Systems Standard and Minimum Recordkeeping Metadata Requirements Standard.

### **Principle 4: Disposal processes of contracted information assets are specified**

All information assets made or received by a contracted service provider must be disposed of in accordance with the SR Act or other relevant legislation and the Disposal Standard.

#### **Behaviours**

Agencies must:

- » only dispose of information assets in accordance with the SR Act and Disposal Standard, including those in the custody of an ASP
- » ensure transfer of ownership of information assets is managed via a current TOCS approved by the State Records Council
- » ensure the contract contains arrangements for the management of the physical destruction of information assets (either by the agency or the contracted service provider)

- » ensure that the contracted service provider maintains documentation for information assets that have been destroyed by the contracted service provider on behalf of the agency.

### **Principle 5 Access to information assets is guaranteed**

Agencies need to ensure that it is possible to recover, or have access to information assets, that are needed by the agency for legislative and business purposes. This includes the provision of access to information assets under the FOI Act and any other legislative access requirements specific to the business of the agency.

#### **Behaviours**

Agencies must ensure:

- » arrangements are made between the agency and the contracted service provider concerning access to information assets including access conditions relating to information assets owned by:
  - the agency but in the custody of the contracted service provider
  - the agency and in agency custody but to which the contracted service provider requires access
  - the contracted service provider, but to which the agency may require access
- » the contract provides that the agency is able to comply with any legislative requirements for access, including FOI and any other legislative instrument that requires or restricts access through the inclusion of access conditions and rights
- » access conditions and rights established under the contract are applied consistently and equitably.

### **Principle 6 Storage requirements are specified**

Information assets must be protected, secure and accessible for as long as they are required to meet the agency's business and accountability needs and the community's expectations.

#### **Behaviours**

Agencies must:

- » determine the degree and detail of documentation required in relation to the storage of information assets in the custody of the contracted service provider
- » ensure the information assets are stored in such a manner that they can be easily retrieved, this includes migrating digital information assets as systems, software and media are upgraded as it becomes obsolete, to ensure the information assets remain accessible for as long as required
- » ensure contracted service providers have an incident management plan that includes recovery of information assets
- » ensure that information assets are handled appropriately for their format and protected from physical harm.

### **Principle 7 Security measures are specified**

Agencies must ensure that information assets owned by the agency are sufficiently protected by storage methods, equipment and handling procedures, incident management plans and security measures, including physical, personnel, cyber and digital.

State government agencies must comply with the South Australian Protective Security Framework and the South Australian Cyber Security Framework in relation to implementing security measures. This obligation extends to contracted service providers.

### **Behaviours**

Agencies must ensure:

- » that security measures implemented by the contracted service provider to protect areas or systems in which the information assets are stored, are appropriate to the security classification of the information assets in accordance with the current government security standard
- » there is protection against unauthorised access to the information assets
- » the tender and contract documents include reference to the current government security standard for security protective measures
- » the contracted service provider has procedures and appropriate technology measures in place to ensure the protection of information assets in the event of a physical or technological accident, emergency or incident, that are relevant to the degree of risk in the event of damage or loss

## **Principle 8 Monitoring and auditing processes are established**

Monitoring of the contracted service provider's information management practices so that action can be taken by the agency to ensure the provider meets their contractual obligations.

### **Behaviours**

Agencies must:

- » specify and document the monitoring and auditing processes in the contract appropriate to the risks of the information assets
- » consider the frequency and method of which monitoring of the control system will be conducted.

## **Principle 9 Post completion information management obligations and requirements are specified**

Agencies must ensure that the completion and post completion stages of the contract in relation to information management are well regulated, monitored and specified in the contract. This includes situations where the contract is extended or renegotiated with significantly different conditions.

Information assets returned to the agency by a contracted service provider at the completion of a contract need to remain accessible and useable (in a readable format).

### **Behaviours**

Agencies must, within the contract, specify:

- » when the information assets will be returned – either at the completion of the contract or periodically over the course of the contract
- » the process for returning the information assets
- » the process for the safe return of all equipment / technology dependent records, including digital copies of information assets on networks, disks, tapes.

Need further assistance?

**Contact**

Position Title

**Tel** (+61 8) 8343 6800

**Email**

**Web** [www.archives.sa.gov.au](http://www.archives.sa.gov.au)

Date approved	Approved by	Date for review	Version
21042023	Director of State Records of South SA	12/04/2024	Final v 1.3