Contracting and Information Assets

Guideline

Version: 1.2

Date Finalised: 21/04/2023

Date for Review: 30/06/2024

STATE RECORDS
of South Australia

Government of South Australia
State Records

Table of Contents

Contracting and Information Assets Guideline

Introduction

Section 13 of the *State Records Act 1997* (SR Act) requires that every agency must ensure information assets in their custody are maintained in good order and condition.

Business activities carried out by a contracted service provider do not diminish your agency's responsibility to ensure your information assets are managed adequately. This obligation extends to the contracted service provider regardless of the custody arrangements.

Purpose and scope

The Contracting and Information Assets Guideline (Guideline) has been developed to support your agency to meet your information management requirements under the SR Act when contracting out your information assets or responsibilities / functions.

The Guideline is applicable to all agencies as defined in section 3(1) of the SR Act and the information assets of those agencies. While it does not apply to local government or universities, it is considered best practice.

In this Guideline, the term 'information asset' incorporates the definition of official record as defined by section 3(1) of the SR Act, and includes 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' means a third party that enters into an agreement with your agency to provide goods and / or services required by your agency for its operations.

This Guideline supports the *Contracting and Information Assets Standard* (Standard) and the *Information Management Standard*, which have been issued under section 14 of the SR Act.

Application of the Standard when contracting with service providers will ensure your agency considers its information management obligations under the SR Act, the *Freedom of Information Act 1991* (FOI Act) and the Premier and Cabinet Circular 012 – Information Privacy Principles Instruction (IPPIs).

Contracting Out

To ensure that the accountability and efficiency of agency and government administration is not diminished as a result of contracting, your agency must ensure that its contracting arrangements include information management practices that meet the government's legislative obligations and requirements.

Tender and contract documentation must include details of the relevant information management requirements the successful contracted service provider will be expected to operate under. Your agency needs to be confident that the successful bidder can meet current legislative and policy requirements before entering into a contract.

Your agency must ensure that adequate information management planning has been undertaken and is well documented prior to finalising any contractual arrangements. This planning should include consideration of information management terms and

conditions for inclusion in the contract in addition to the services to be provided. This becomes more critical when dealing with sensitive or personal information.

If your agency does not consider including information management arrangements during the planning process, and in the agreements and contracts, you may find it difficult or impossible to reacquire information assets when needed for administrative or legislative purposes.

To ensure your agency meets your information management obligations, 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
9. Post completion information management obligations and requirements are specified

Implementation of this Guideline

This Guideline can be applied where your agency is planning to enter into a contract where a service is to be undertaken on behalf of your agency, and ownership and legal possession of the information assets associated with the service remains with your agency. This includes:

- those services that could have previously been considered core functions of your agency, (such as case management), or
- where information assets are required to be provided to the contracted service provider by your agency to enable them to effectively provide the service.

It does not apply to:

- the sale or privatisation of agency enterprises or activities (where ownership and custody of information assets is transferred, referred to as TOCs) or
- grant-funding relationships.

This Guideline can be used by procurement staff, contract managers, records managers, legal practitioners, senior management and other stakeholders involved in the contracting process.

This Guideline is not intended to constitute legal advice. Your agency is advised to seek legal advice when entering into contractual arrangements.

Model terms and conditions have been developed by the Crown Solicitor's Office to assist agencies to meet their information management obligations and are available on the State Records website.

While the Standard and Guideline aim to assist your agency when planning for any contractual arrangement, there may be instances where their application is limited or unnecessary.

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.

Risk Assessment

The risk assessment should be conducted and documented in accordance with your agency's risk management framework. Refer to the *Information Governance Guideline* for more information regarding how to access levels of risk.

The likelihood of the risks identified occurring should be mitigated by including relevant information management provisions, such as defining ownership of the information assets and specifying how they will be disposed of, in the contract.

Consultation and research

As part of the risk assessment your agency should consult with all relevant bodies or parties that may have the knowledge and experience necessary to ensure the tender and contract documentation contains the appropriate inclusions. Parties to consult include:

- your agency's:
  - **Records Manager** – who can provide advice on the information assets that are created by your agency in relation to the function or activities to be undertaken by the contracted service provider. They may be able to offer advice in relation to the application of the principles of the Standard and in ensuring your agency can continue to meet the requirements of the Standard and the SR Act
  - **Privacy Officer** – who can offer advice in relation to the privacy implications of contracted service providers having access to personal information and the kinds of protection that the contracted service provider must have in place to ensure those kinds of information assets in the custody of the contracted service provider are not exposed to unacceptable levels of risk
  - **Accredited FOI Officer** – who can offer advice in relation to the effect of contracting on the efficient operation of the FOI process within your agency. In the case of information assets being transferred to the custody of the contracted service provider your agency must ensure that your agency is able to meet its legislative obligations in relation to the FOI Act
  - **accredited purchasing unit and contract management staff** – while these staff will already be involved in the contracting process, they may be able to offer advice in relation to the manner in which the tender and

contracting process is handled and the kinds of documents that will be created as a result of the contract

- the **Crown Solicitors Office (CSO) or other appropriate Legal Counsel** – will be able to offer advice in relation to the tender and contract documents in their entirety. The CSO can also offer specific advice in relation to information management terms and conditions.

Trans-border data flow

Trans-border data flow is defined as the flow of data from an entity in one jurisdiction to an entity in another jurisdiction.

In some instances contracts may be awarded to contracted service providers, which results in information being transmitted from one state or country to another which may have different access and privacy regimes to South Australia.

Any risks with trans-border data flow need to be identified, documented and mitigated where possible, by your agency prior to signing the contract. Risks include whether the or access laws of the other jurisdiction will allow it to obtain access to your agency's information assets, including those containing personal information, with or without your knowledge.

The community has a right to expect that the information they have given, or may be required to give, will not be exposed to an increased level of risk as a result of contracting decisions that have been made which are out of their control. Therefore, it is important that your agency ensures that in cases where personal information is transmitted or made available to other entities in other jurisdictions as a result of contracting, that procedures are in place to ensure the information is protected.

Where information, in particular personal information, will be transmitted to another jurisdiction (for example to be stored in a cloud located overseas), your agency should seek specific advice from the Crown Solicitors Office or other appropriate Legal Counsel to ensure the protection of that information through contractual terms and conditions.

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.

Your agency should ensure the contract specifically identifies all information assets that remain the property of your agency, including those created during the contract. Your agency should continue to own and legally possess all information assets made or received in order to maintain transparency and accountability.

Ownership

Prior to commencing the tendering process, your agency must determine which information assets arising out of, or in connection with, a contract should be owned by your agency or the contracted service provider. All ownership decisions/agreements must then be clearly specified within the contract.

If no tendering is required, information asset ownership must also be clearly specified in the contract.

Under the Information Management Standard, your agency is required to ensure:

- ownership is assigned, this includes assigning ownership in contracts (Behaviour 3.1), and
- that information asset owners are aware of their responsibilities and accountabilities for managing information assets (Behaviour 3.2).

Your agency retains legal possession of any information asset it provides (transfers) to a contracted service provider to enable it to perform a service. The contract should also require those assets to be returned upon completion of the contract or at another specified date to your agency.

In order to determine ownership of specific information assets created by your agency and the contracted service provider, it may be useful for your agency to consider the following questions:

1. does the function or business activity to be undertaken by the contracted service provider represent services performed on behalf of your agency? For example is there evidence of a core function of your agency, is the service provided as a result of a legislative or regulatory responsibility of your agency, or is the service provided by the contracted service provider provided directly to your clients?
2. would any information assets involved in the contractual arrangements be required by your agency (or another contracted service provider) at the termination of the contract, to enable the service delivery to continue or for another other reason?
3. would the information assets need to be referred to by your agency for any reason, be used to establish the rights, entitlements or obligations of your agency or an individual, or be used for ongoing research?

4. would your agency need access to these information assets for any purpose either during or after the contract? For example for access under FOI?

If you answer yes to **any** of the above questions, ownership of the information assets should be vested with your agency.

If you answers no to **all** of the questions, then ownership of the information assets could be vested with the contracted service provider. Contract State Records for more information regarding transfer of ownership and custody to a third party.

Custody

For the contracted service provider to undertake the function or business activity being contracted out it may be necessary for some information assets to be transferred to the custody of the provider. Prior to transfer, you must determine which information assets your agency needs to retain legal possession (ownership) of.

Legal possession and custody are two separate issues. Whilst it may be necessary for legal possession to be with your agency, custody can still be vested with the contracted service provider. In many cases it will be impossible for the contracted service provider to undertake the function or business activity without a transferral of physical custody.

For information assets:

- which contain sensitive or security classified information, or
- where disclosure would result in a breach of confidence or prejudice any continuing action

your agency should consider retaining custody of the information assets.

If it is necessary to transfer selected records, then it is essential to ensure that the information is suitably protected in accordance with Standards issues under the SR Act, the South Australian Protective Security Framework (SAPSF) and the South Australian Cyber Security Framework (SACSF). In some other cases it may be necessary for your agency to retain custody and to allow for access to the information assets by the contracted service provider as required and under whatever conditions your agency deems appropriate.

Permanent or temporary value

Your agency can identify the information assets designated as permanent value by inserting a list of these information assets in the contract. **Note:** all permanent value information assets must remain in the legal possession of your agency.

A permanent value information asset is one that has archival value and will be retained permanently for research by the general community subject to appropriate access restrictions.

A temporary value information asset is one that does not have archival value and may be destroyed when a prescribed retention period has elapsed.

Transfer of ownership of information assets

Where ownership of the information assets has been determined to belong with the contracted service provider, your agency must ensure a Transfer of Ownership and Custody Schedule (TOCS) is in place.

Transferral of ownership of information assets constitutes a 'disposal' as defined by the SR Act, requiring a disposal determination issued by the Director of State Records and approved of by the State Records Council. The TOCS represents this approval.

In the event a TOCS is not in place your agency must contact State Records for further assistance before transferral of ownership of any information assets can occur.

Transfer of custody can occur without the use of a TOCS. Therefore, in the event that transfer of ownership of information assets cannot occur immediately, the transfer of custody can still occur to ensure continuity of service.

Note: transferral of ownership can include transferral from your agency to a contracted service provider and from a contracted service provider to your agency.

Intellectual property rights

Intellectual property is defined as an idea that can be protected by law once it has taken a tangible form, for example the idea has been documented or recorded in some way. Intellectual property of any kind must be written down in order to be properly protected by copyright legislation.

Ownership of the intellectual property contained within the information assets created during the contract should be clearly defined as well as ownership of existing information assets. Your agency must ensure that it owns the intellectual property rights in all information assets, existing and those to be created, that relate to the contract.

Transfers of permanent value information assets

Transferral of custody of information assets of permanent value in a contract does not include transferral of legal possession. Information assets of permanent value cannot be legally transferred to a contracted service provider.

However, in some cases the physical transferral of custody of information assets of permanent value to a contracted service provider may need to occur.

The most common ways in which information assets can be determined as having a permanent value are via legislation or by application of an approved disposal schedule (including General Disposal Schedules (GDS), Records Disposal Schedules (RDS), and TOCS).

Serious consideration should be given to the transfer of custody of information assets that are either very old, very fragile or both. Your agency should carefully consider the risk of loss of the information assets to your agency against the benefit of custody of the information assets being transferred to the contracted service provider.

In these situations your agency should consider providing copies of the information assets to the contracted service provider rather than the original information assets to meet the needs of the contracted service provider in service provision and ensuring the preservation of the original information assets.

Alternatively in some cases your agency may decide to retain these types of information assets in their own custody and provide access of the information assets to the contracted service providers as required.

In all cases where information assets are transferred to the contracted service provider your agency should stipulate the conditions they expect the information assets to be kept in to ensure the information assets are protected and are returned safely to your agency at the completion, termination or other stage of the contract (refer to Principle 6: Storage and Principle 7: Security for further information).

Your agency should also be aware that contracted service providers may be creating information assets of permanent value associated with or because of the contract. In these cases you should stipulate the conditions the contracted service provider is required to keep those information assets in to ensure they are protected prior to their transferral to your agency at the termination or completion of the contract or any other time as determined in the contract.

Principle 3
Creation and control requirements are specified

All information assets to be created under the contract must be documented in the contract and managed appropriate to risk and in accordance with the SR Act.

Information assets contain the evidence of actions taken, decisions made, procedures enacted and policies developed by your agency. They are essential for proving what was said, done or approved. Therefore, your agency is required to create information assets to ensure the outcomes of your business transactions are captured and retained that can be relied upon and trusted.

Information assets are also created when your agency receives documents and they are incorporated into your agency's pool of information assets. As information assets are often the primary source of information for your agency in tracking its business, information assets are created whenever evidence of business activity is required.

Given this importance it is essential that they be captured into information management systems upon creation or receipt in a controlled and systematic manner. An information management system may include, but is not be limited to, electronic document and recordkeeping systems (EDRMS), information management software, a finance management system or even a manual card based system providing its use ensures control of the information assets recorded within it and meets the requirements of the Information Management Standard.

Creation

Many Acts of Parliament administered by agencies require those agencies to create information assets in specific circumstances or for specific purposes. While the contract may require the contracted service provider to create those documents instead of your agency, it remains your agency's responsibility to ensure those information assets continue to be created appropriately.

If your agency, or contracted service providers, fails to capture information assets you are subject to the following risks:

- inability of your agency to meet other statutory obligations
- financial risk to your agency from the loss of the information asset
- loss of the State's history
- inability to meet community expectations that information assets will be created
- loss of personal information / personal history of members of the community
- poor decision making as a result of incomplete information
- increased corporate risk
- substandard service provision.

Your agency should also note that its responsibilities in the Information Management Standard are not negated because a contracted service provider is now undertaking the creation of information assets on behalf of your agency.

Therefore, it is your agency's responsibility to ensure that the contracted service provider is aware of what those responsibilities are. The only way your agency can be assured is to identify in the contract any legal requirements for specific information asset creation.

This includes ensuring that the contracted service provider is aware that they will be involved in the creation of information assets of permanent value. Whilst these kinds of information assets may not be identified as such at the time they are created, contracted service providers should be made aware that at some point those information assets may be identified as having a permanent value and will need to be treated accordingly.

By specifying your agency's legal requirements regarding the creation of information assets in the contract, your agency will meet the following behaviours in the Information Management Standard:

- behaviour 1.2 – identify and document what their information assets are, where they are stored and who is responsible for their management
- behaviour 2.1 – analyse and document what information must be created and managed across the organisation applicable to the regulatory environment in which your agency operates, and
- behaviour 2.3 – assess the risks of not creating or managing information where there is a legal, evidential, or business need.

Control

It is important to ensure that the control systems for agency owned information assets are established by the contracted service provider prior to the provider being made responsible for the custody of those information assets.

Controls for information assets should include:

- creation (where this occurs inside the system), capture and classification
- access, retrieval and use (including security and personnel security requirements)
- storage and preservation, including preservation of legibility
- control of changes (such as version control and audit trails)
- retention and disposal.

If such control systems are not established your agency runs the risk of potentially losing a valuable asset.

Your agency should bear in mind that you are required to meet other statutory obligations outside of the SR Act. For example, the FOI Act will require your agency to locate any information assets required to process an application made under that Act. Whilst physical possession may have passed to the contracted service provider for agency owned information assets, legal possession has not.

Therefore, if the contracted service provider does not have the appropriate control mechanisms in place prior to the transferral of custody of information assets, your agency may find itself in a position where it is unable to meet its legislative obligations. In addition, your agency will not be able to meet Principle 5 of the Information Management Standard: Information is available as required.

Managed appropriately

Your agency must ensure that all information assets created, generated or received by the contracted service provider are managed appropriately.

It is important that the contracted service provider is made aware that the control systems they have in place to manage information assets that are transferred into their custody should be utilised for any information assets created, generated or received by the contracted service provider regardless of its format.

It is essential that the information assets are captured into information management systems upon creation or receipt in a controlled and systematic manner. Your agency should ensure that information assets are classified and stored using a classification system based on its business functions and activities that aligns with your GDS or RDS rather than a subject based or organisational structure-based classification.

In doing so your agency will meet the following behaviours of the Information Management Standard:

- behaviour 1.2 – understand and document how your information assets support your business objectives and operations or compliance obligations, and
- behaviour 1.3 – ensure information assets are linked to your agency's business functions and activities.

The contracted service provider should also recognise that the information assets in their custody, whether existing or created during the life of the contract, should be managed in a discrete system separate from the information assets owned by the contracted service provider.

Compliant systems

Compliant systems are format and technology neutral. Systems may be:

- physical in nature (such as hardcopy filing systems) or
- digital (such as business information applications or dedicated Electronic Document and Records Management Systems (EDRMS)).

Having compliant systems will help ensure the quality and authenticity of information assets as well as ensuring they are managed and stored appropriately and remain accessible for as long as required.

All compliant systems must be designed and implemented in accordance with the:

- Managing Digital Records in Systems Standard (Systems Standard)
- Minimum Recordkeeping Metadata Requirements Standard, and
- Information Management Standard.

The obligation to use compliant systems extends to the contracted service provider.

For a system to be compliant is must meet the **minimum** functional requirements established in the Systems Standard, which include:

- being able to store digital information assets required as evidence of business activity as a record
- ensuring information assets can be located and read
- being able to apply access permissions to information content and metadata
- ensuring information assets can only be deleted through an authorised process.

For a full list of the minimal functional requirements a system must have, refer to the Systems Standard (Note this Standard should be used / read in conjunction with the Minimum Recordkeeping Metadata Standard as business systems need to hold the most up-to-date information while recording the relevant metadata to show the exact state of the data on which decisions were made at a particular point in time).

Principle 4
Disposal processes of 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, other relevant legislation and the Disposal Standard.

Your agency must only dispose of information assets in accordance with an approved disposal determination under section 23 of the SR Act.

A determination provides authorisation for information assets to be destroyed or transferred to non-government entities and comes in the form of either a GDS, RDS or a TOCS. For more information on TOCS refer to Principle 2.

Your agency needs to have appropriate disposal coverage in place irrespective of whether your agency's information assets are administrative or operational.

There are several GDS specifically designed to cover state and local government agencies. GDS 30 prescribes the disposal of administrative information assets for all state government agencies and GDS 40 prescribes the disposal of administrative information assets for local government authorities.

However, for information assets created that are unique to your agency, these require a current RDS approved by the State Records Council to dispose of your operational information assets.

You should consult with your agency's Information Manager to determine which disposal authorities are applicable to the classes of information assets affected by the contract. (For further information in relation to the application of GDS 30, GDS 40 or an agency specific RDS, your agency should seek advice from State Records.)

Additionally, some South Australian legislation contains specific retention, disposal or other information assets management provisions. Your agency must be aware of any such legislative requirements and its statutory responsibilities.

Disposal is authorised

Unauthorised destruction of information assets is an offence under section 17 of the SR Act. The result of which may leave your agency open to litigation, financial loss and political embarrassment.

To ensure information assets are disposed of systematically and in accordance with the SR Act and Behaviour 5.5 of the Information Management Standard, the Disposal Standard should apply. The Disposal Standard sets out the mandatory principles and requirements your agency must adhere to when disposing of government information regardless of the custody arrangements.

Your agency needs to determine whether the contracted service provider will be responsible for destroying information assets or return the information assets to your agency and in what condition, to enable your agency to manage the physical destruction process.

The retention period outlined in approved disposal schedules is the minimum period that information assets need to be retained for. Your agency may decide to keep

specific information assets for longer than the minimum retention periods outlined in the schedule. Your agency can make these determinations in accordance with the Disposal Standard.

Disposal is managed

It is vital that the contract contains arrangements for the physical destruction of information assets if to be carried out by the contracted service provider. The Disposal Standard applies regardless of custody arrangements. It is up to your agency to determine whether to allow the contracted service provider to manage the physical destruction process. Responsibility for managing the physical destruction of information assets should be clearly documented in the contract.

Under the Disposal Standard, your agency must ensure that its contracted service providers are:

- aware of their responsibilities for the retention and disposal of information assets, and
- appropriately skilled and have the capacity to undertake disposal tasks.

It is also important to note that the disposal of information assets by a contracted service provider occurs in accordance with an approved disposal schedule and with the approval of your agency. A breach of section 17 of the SR Act, which refers to the intentional damage, alteration or disposal of information assets without authority, carries a maximum penalty of $10,000 or two years in prison.

Your agency is responsible for reporting a breach of section 17 of the SR Act to the attention of the Manager [Director] of State Records as soon as your agency becomes aware.

Disposal is accountable

State Records recommends your agency considers the risks associated with having a contracted service provider manage the physical destruction of information assets owned by your agency. It may assist your agency in ensuring that information assets owned by your agency and in the custody of the contracted service provider are not knowingly or inadvertently destroyed by the contracted service provider if your agency manages the destruction process.

Under the Disposal Standard, your agency must maintain documentation of all information assets held, including evidence of all information assets disposed of by destruction (by your agency or a contracted service provider) or transferred (to either State Records or under a TOCS).

For a list of risks associated with having the contracted service provider manage the physical destruction of information assets owned by your agency, refer to creation under Principle 3.

However, if after considering these risks your agency chooses to allow the contracted service provider to manage the physical destruction process it must be managed in accordance with the requirements of the SR Act and the Disposal Standard.

Principle 5
Access to information assets is guaranteed

Information assets are not only retained for their administrative use but also to meet legal and community requirements and expectations. Your agency needs to ensure that it is possible to recover or have access to information assets that are needed by your 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 your agency.

Your agency should also consider that the contracted service provider may need access to information assets held by your agency to ensure continuity of service.

Access to information assets and the disclosure of information within them needs to be systematic, considered and consistent. The indiscriminate release of, or refusal to release, information may infringe on the rights of individuals or the state and cause severe liabilities for your agency.

Information contained within the information assets may require disclosure control for reasons of security, personal privacy, state-to-state, and state to foreign nation security, commercial confidentiality or legal liability.

However, despite these reasons for disclosure control, access to the public must remain the same regardless of who is delivering the service where ownership of the information assets remains vested with your agency. If ownership of the information assets has been transferred from your agency, you may have limited or no control over disclosure of the information.

Access arrangements

Your agency must ensure arrangements are made in the contract concerning access to information assets related to the business activities undertaken by the contracted service provider on behalf of your agency regardless of ownership.

The following arrangements must be specified in the contract (where applicable) access conditions relating to information assets owned by:

- your agency but in the custody of the contracted service provider. The information assets remain in the legal possession of your agency. Your agency has the same access rights to their information assets as they would if the assets were within your agency's physical possession. The contracted service provider should be made aware that they cannot impede your agency's access to those information assets in any way. This includes having inappropriate or inadequate control systems resulting in information assets not being able to be located.

  To ensure ongoing access, your agency will need to:

  - assign responsibility for providing access to information assets and disclosing the information they contain. Where the information assets are in the custody of a contracted service provider the responsible person for the provision of access should still be employed by your agency

- develop criteria for assessing requests for access to, and disclosure of information within information assets, where other legislative processes do not apply, for example the FOI Act
- identify and document security issues governing the release of information within your agency's information assets; ensure that it has processes in place to ensure access to information assets does not compromise the reliability of the information assets
- identify and document any commercial confidentiality agreements to which it is a party governing the release of information within your agency information assets, and
- have processes in place to seek legal advice where the provision of access to and the release of information from your agency information assets is likely to expose your agency to legal liabilities.

» and in the custody of, your agency, but to which the contracted service provider requires access. In some cases the contracted service provider may require access to information assets owned by and in the physical possession of your agency to ensure continuity of service by the contracted service provider. In these cases arrangements for the temporary transferral of those information assets will need to be made or arrangements for the contracted service provider to be able to view the information assets at your agency.

  If the information assets are to be transferred, your agency should determine an appropriate time for the information assets to be returned to your agency. In determining these arrangements your agency should consider the reasons why the information assets were not transferred to the custody of the contracted service provider at the time the contract was made and determine if those reasons have any bearing on the decision being made now.

» the contracted service provider, but to which your agency may require access. In limited cases your agency may require access to information assets owned by the contracted service provider. It would be highly unlikely that your agency would require access to information assets of the contracted service provider that do not relate to the business activities that have been contracted out. In these cases it would be up to the discretion of the contracted service provider as to whether your agency could be granted access. If continued access to the information assets is required, including those created by the service contract provider, ownership should remain with your agency.

Legislative requirements for access

Compliance with legislative requirements for access does not change because the custody arrangements for agency information assets has changed, even as a result of the contractual arrangement. Therefore, if your agency enters into contracts which involves the transfer of custody of information assets to the contracted service provider, you must ensure you are able to continue to comply with the legislative requirements for access, including FOI and any other legislative obligations.

The only time that the legislative responsibilities of your agency will change in relation to access provisions in relation to information assets arising out of or in connection to a contract is when legal possession is changed via the use of a current TOCS approved by the State Records Council.

Accessibility

Information assets must remain accessible and in good condition (if digital, in a readable format) for as long as they are required. This includes when information assets need to be migrated from a physical to a digital format for preservation or conservation purposes, or digital information assets need to be migrated from one system, software or media format to another due to upgrades or the system becoming obsolete (Information Management Standard, Behaviour 5.3).

For example, if an information asset covered by a GDS has a retention period of 100 years it must remain accessible over the entire 100 year period and be capable of being relied on as trusted and authentic evidence of your agency's decisions made and actions taken. This means it must be capable of being retrieved by your agency in a readable format.

If records have a retention period longer than seven years, it is likely that they will need to be migrated from one application to another as software or hardware is upgraded, replaced or becomes unsupported.

The migration process requires analysis of both the creating and the receiving applications and must be carefully documented, well tested and any compromises or risks agreed between your agency and the contracted service provider. Because no two applications will be identical, some data will be lost. This needs to be documented and agreed.

Access conditions and rights

Any rights established under the contract must always be applied consistently to ensure the contract is honoured.

Access conditions and rights to agency owned information assets in the custody of the contracted service provider established under the contract must be protected. Where a dispute exists or arises between your agency and the contracted service provider, the contracted service provider must acknowledge that it has no right to withhold information assets from your agency.

For State government agencies, access to personal information by the subject holder must also be specified in the contact in accordance with clause 5 of the Department of Premier and Cabinet Circular Information Privacy Principles Instruction (IPPI or PC012). PC012 regulates the way state government agencies manage, collect, use, disclose and store personal information.

Principle 6
Storage requirements are specified

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

To lessen the likelihood of loss or damage to information assets whilst in the custody of a contracted service provider, your agency should ensure that storage arrangements are included in the contract.

It is also vital that the contract include arrangements for any ongoing storage of information assets at the termination or completion of the contract. Failure to do so may result in information assets being destroyed or misplaced through the perception that they are no longer the concern of the contracted service provider. It is important, however, that along with arrangements for ongoing storage of information assets, the contract establishes the date or timeframe for information assets to be returned by. The reason for this is two-fold. It ensures that the information assets aren't subject to extended periods of risk but also ensures contracted service providers aren't left with the burden of storing information assets that are no longer their responsibility. Refer to Principle 9 – Contract Completion for more information.

Storage of non-current information assets of temporary value must be managed in accordance with the Management and Storage of Temporary Value Information Assets Standard.

In relation to the storage of information assets of permanent value by contracted service providers, the contracted service providers must be made aware that information assets of permanent value are to be transferred to State Records after they are 15 years old and are no longer required for administrative purposes in accordance with the Transfer of Official Records Standard.

Documentation required

The degree and detail of documentation required in relation to the storage of information assets in the custody of the contracted service provider will depend on a number of variables, including:

- the size of the business activity being conducted by the contracted service provider
- the amount of information assets transferred to the custody of the contracted service provider, and
- the sensitivity of the information assets being transferred.

In determining the degree and detail of documentation required of a contracted service provider, your agency should consider the degree of storage documentation they required when you were responsible for the business activity. It would be unwise for your agency to require less of the contracted service provider than your agency would require of itself, bearing in mind that your agency no longer has physical control of the information assets.

Information assets must be easily retrieved

Where legal possession for information assets remains with your agency, the requirement to provide access is the same as if those assets were still in your agency's custody.

Your agency must ensure that the information assets in the custody of the contracted service provider are properly indexed and ordered in a form that will enable your agency to carry out proper inspections of the information assets (where necessary) and can easily retrieve them if required (for example to respond to an FOI application). Inadequate documentation may expose your agency to unacceptable risks and costly consequences.

Consideration should also be given to requiring the contracted service provider to provide the following kinds of information in an agreed format in relation to storage of information assets:

- where information assets are stored
- the number and title of files created over a specified period, including the number of volumes opened for each file
- up-to-date location reports
- the number and title of files transferred to temporary or off-site storage facilities.

In determining the kinds of information your agency requires, consider the kinds of information your agency collects or uses that is derived from their own information management system.

Incident Management Planning

The physical security of information assets is important. Your agency must ensure that information assets, which are the property of your agency but stored with a contracted service provider, are sufficiently protected by storage methods, equipment and handling procedures, incident response plans and security measures.

Information assets are always potentially at risk of an incident. Due to the importance of information assets, their loss may be crippling for your agency depending on the significance of the information assets damaged or lost.

Incident management is part of wider risk management and mitigation strategies that your agency should pursue, regardless of whether the information assets are in the custody of your agency or the contracted service provider.

Incidents affecting storage may include:

- natural events such as earthquakes, cyclones, bushfires, floods, vermin
- structural or building failure such as malfunctioning sprinklers, heating or air conditioning systems, roof leaks
- industrial accidents such as nuclear or chemical spills, gas leaks, fire
- technological incidents such as viruses and computer equipment failures
- criminal behaviour such as theft, arson, espionage, vandalism, riots and terrorism, and war
- accidental loss through human error.

The contract should specify that the contracted service provider has the relevant incident response plans implemented in accordance with the degree of risk to

information assets in the event of damage or loss. Refer to the Recordkeeping Management Disaster Planning Toolkit at State Records website.

Handling of information assets

The tender and contract documents need to include a minimum standards for the storage of information assets.

Information assets in all formats are likely to deteriorate if they are not handled appropriately. Personnel may be injured if appropriate occupational health and safety considerations are not taken when handling information assets. Your agency should specify the correct handling, use or transport of information assets to minimise the risk of personal injury and to ensure the preservation of information assets for as long as they are required regardless of where those information assets are located.

Your agency should also consider including the following:

- development of handling procedures for the general use of information assets as well as for information assets in transit. These can be used as the basis for the expectations they have for the handling of information assets in the custody of the contracted service provider
- forbidding smoking, eating or drinking in or near information assets and information assets storage areas
- ensuring containers are clean and in good condition, designed to fit the information assets, strong enough to withstand handling, pressure and the weight of the information assets, and of a quality and composition commensurate with the information assets format, media and use
- identification and removal to a new location of information assets stored in dangerous formats. These information assets should be moved to a location away from information assets that could be affected by fumes, etc
- raise shelving off the floor by 85-150mm as an incident precaution
- establish and maintain incident management programs and an up-to-date incident response plan – ensuring all storage areas have alarms, heat and smoke detection, and fire extinguishing equipment
- equipment complies with occupational health, safety and welfare codes of practice.

Principle 7
Security measures are specified

Information assets owned by your agency must be sufficiently protected by storage methods, equipment and handling procedures, incident management plans and security measure, including physical, personnel, cyber and digital.

Information is a vital asset to the state government and as such needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and the successful achievement of objectives.

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

Information security is achieved by implementing a suitable set of controls including policies, standards, practices, procedures, organisational structures or software functions.

Your agency should consider the following in relation to information security:

- how the legal requirements are to be met (eg data protection and legislation)
- what arrangements will be in place to ensure that all parties involved are aware of their security responsibilities
- how the integrity and confidentiality of your agency's information assets are to be maintained and tested
- what physical and technological controls will be used to restrict and limit access to authorised users to the agency's sensitive or personal information
- what levels of physical security are to be provided for information assets
- the right of audit (see Principle 8 for more information).

Agencies should also ensure that any personal information in the custody of the contracted service provider is handled in accordance with the PC012 or the SA Health Privacy Policy as used by the Department of Health and Wellbeing.

In the event of inadequate security measures or contracted service provider negligence resulting in the loss or destruction of information assets, the contracted service provider should be required to pay all costs incurred by the agency reinstating those information assets.

Further information on the physical security of information assets can be found in the Management and Storage of Temporary Value Records Standard on the State Records website.

Information assets are stored appropriate to their security classification

In the instances where information assets are in the custody of the contracted service provider your agency should ensure the contracted service provider implements the same security measures your agency is required to implement appropriate for the

security classification to the information assets. This ensures compliance with Behaviour 5.1 of the Information Management Standard.

Your agency should refer to the Information Governance Guideline, the SAPSF and the SACSF for more information on security classifications.

Unauthorised access

Information assets are an essential part of your agency's business. Information Management systems and storage facilities need to be designed and implemented to protect information assets from unauthorised access, alteration, deletion or loss.

Your agency will need to ensure that the information management systems and facilities used by the contracted service provider are adequate for the information assets that are being managed throughout the course of the contract.

Protecting unauthorised access to physical information assets may include the use of storage rooms that are secured by a set of procedures such as security swipe cards, sign-in sheets or security keys that only authorised staff have access to. Protection of digital information assets might require the placement of databases or terminals in secure rooms or include functionality that allows information management staff with appropriate access to apply caveats to prevent unauthorised access to electronic information assets.

Your agency may need to decide what level of security is required as appropriate to the security classification of the information assets that the contracted service provider will be required to meet.

Control measures appropriate to risk

One of the major threats to the safety of information assets is the risk of incident. Counter incident management strategies yield many benefits for information assets.

The contract should stipulate the contracted service provider should be required to undertake a risk assessment relevant to information assets storage facilities and recordkeeping systems, and the development of subsequent plans to reduce the probability of incident and loss; activities to identify and protect vital information assets; and the development of incident response and recovery plans to follow after an incident.

Further information in relation to the physical protection of information assets can be found under Principle 6 – Storage.

Risk audits should also be applied to digital information assets and their locations. Existing security procedures should be examined and documented. Additional risks common in digital formats such as disk crashes, hardware failure and system crashes should also be examined.

The SAPSF should be consulted by your agency when specifying what procedures and technology measures are required of the contracted service provider.

Principle 8
Monitoring and auditing processes are established

Monitoring of the contracted service provider's information management program ensures that action can be taken by your agency to ensure the provider meets their obligations under the SR Act and the Standard.

The most effective method to measure compliance is to periodically inspect the information assets held by the contracted service provider through an appropriate reporting regime established in the contract. It is important that the contract establishes your agency's right of access to information assets for the purpose of monitoring performance. Specific advice will need to be sought in relation to contracts with offshore companies as monitoring and audit arrangements that include a physical inspection component may not be possible.

Frequency and method of auditing / monitoring

Your agency must provide the contracted service provider with details of what will be audited or monitored and provide sufficient warning of when these occur. Specific details of the content of the audit or monitoring exercise do not need to be included in the contract. However, the frequency of the exercise should be determined and included.

Your agency should consider making it mandatory for the person to whom responsibility for the information assets has been assigned, be in attendance during the process.

Other considerations for your agency to assist in the monitoring and audit process include:

- ensuring information assets of permanent value are transferred to the custody State Records upon completion of the contract or when no longer administratively required
- ensuring information assets of permanent value have been returned to your agency upon completion of the contract or when no longer administratively required
- provision of up-to-date location reports prior to an audit being undertaken to enable your agency to match the report against control information assets kept by your agency. This will ensure an audit can be undertaken on all information assets that exist
- your agency could consider the determination of a performance indicator that the contracted service provider must meet e.g. 80% of information assets were in the location specified on the location report provided by the contracted service provider.

The above list is not exhaustive. Your agency should include any other requirement you feel is necessary to ensure an effective audit can be undertaken and which gives your agency enough data to be satisfied the contracted service provider is meeting your information management requirements.

Periodical reports

Your agency needs to ensure that the contracted service provider reports periodically on the control systems of the information assets in the information management system to ensure they are aware of the extent of information management practices being conducted by the contracted service provider.

The nature of these reports and frequency needs to be determined and outlined in the contract. Monitoring control systems of information assets in the information management system will ensure that information assets are being appropriately created and captured. It may be appropriate for your agency's staff to physically view a sample of files in these control systems to ensure the accuracy of the systems and that metadata is being applied adequately.

Failure to monitor

Your agency is responsible for ensuring that contracted service providers are fulfilling their requirements outlined in the contract, including those practices relating to information management.

Monitoring can take a variety of forms including onsite auditing or the development of regular reports by the contracted service provider to your agency. The nature of these reports and onsite audits should be specified in the contract with the contracted service provider.

Without monitoring the contracted service providers' information management practices, your agency cannot ensure that their information management responsibilities are being managed and maintained or that the services being provided by the contracted service provider on behalf of your agency are being delivered adequately.

The risks associated with not monitoring the contracted service providers' information management requirements include:

- your agency:
  - may not meet the behaviours established in the Information Management Standard, potentially leading to a breach of the SR Act (section 16)
  - cannot confirm that the function / business activity that the contracted service provider is delivering on behalf of your agency is being delivered appropriately due to the lack of information being provided
- severe legal liabilities if information assets cannot be located upon request (e.g. FOI, subpoenas)
- increased corporate risks as your agency will not be able to provide evidence to support actions
- substandard client service provision.

Principle 9
Post completion information management obligations and requirements are specified

Your agency 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.

It is unlikely that the contracted service provider will want to devote time and effort to information assets of an activity that it is no longer performing, unless there is a contractual requirement to do so.

Return of information assets

It is most important to determine how the information assets of the business activities undertaken by the contracted service provider will be dealt with at the end of the contract. Failure to communicate agency requirements for the return of agency owned information assets could result in lost information and increased exposure to risk.

It is important that the information assets of your agency in the custody of the contracted service provider, including those existing and those created during the life of the contract, are returned promptly and within a timeframe as specified by the contract. It is the responsibility of your agency to determine whether you would prefer them to be returned at the termination or completion of the contract or earlier. This should also include any relevant control systems used to manage information assets throughout the contract in relation to the delivery of that service. They may include records / document management software, databases, spreadsheets or manual listings. The contract should specify that control information assets, regardless of their form, should be returned along with the appropriate information assets at the completion of the contract.

It is not always necessary to leave the return of information assets until the termination or completion of the contract. In some cases it may be more efficient, or even safer, to have the contracted service provider return information assets in its custody, but not in their legal possession, prior to the end of the contract or indeed periodically over the term of the contract.

One consideration in favour of returning information assets periodically may be that the information assets fall reasonably neatly into regular or periodic timeframes. There may also be other reasons more specific to the kinds of information assets or functions being performed. Returning information assets periodically may also prove more efficient for your agency as staff will not be required to deal with all of the information assets of the contract at once. Rather, they can be dealt with in several reasonable sized sentencing projects that span the life of the contract.

Information assets returned by a contracted service provider to your agency at the completion of a contract need to remain accessible and useable (in a readable format). In the case of digital information assets these will need to be transferred / migrated to a

state government compliant system to ensure the information assets can continue to be used or sentenced appropriately.

Refer to the Managing Digital Records in Systems Standard for more information.

Transfer of permanent value information assets to the custody of State Records must be done in accordance with the Transfer of Official Records Standard. For more information refer to the State Records website.

Process for return

Your agency should stipulate that the information assets need to be returned in a manner in which allows them to be easily reviewed and retrieved by your agency. This means they should be boxed and listed appropriately for your agency to know exactly which information assets are stored in which boxes.

The boxes that information assets are returned in should also be appropriate for their storage. They should be in containers that are clean and in good condition, designed to fit the information assets, strong enough to withstand handling during transportation and of good quality and composition commensurate with the information assets format, media and use. The use of appropriate couriers will also need to be considered, including companies that use vehicles that can protect information assets from rain and other elements during transportation.

Responsibility for payment of couriers or transportation should be considered for inclusion in the contract, remembering that a significant amount of information assets may have been created during the term of the contract.

Return of all equipment / technology

The process of returning information assets should include the return of all equipment and technology dependent information assets in such a manner that those information assets can still be reproduced by your agency. The kinds of information assets to be considered would include digital copies of information assets on networks, disks and tapes. All of which will require specific equipment or software to reproduce. Information assets that are unable to be reproduced due to changes or redundancy of technology are likely to become a liability for your agency that receives them.

Remember, the information assets being returned must remain accessible and in a readable format under the Information Management Standard. It is therefore the responsibility of your agency to ensure they can be reproduced. Including this requirement in the contract is the best way of meeting this responsibility.

Need further assistance?
Tel (+61 8) 7322 7077
Email staterecords@sa.gov.au
Web www.archives.sa.gov.au

Date approved	Approved by	Date for review	Version
21042023	Manager, Information Governance	3006204	Version 1.2