Government of South Australia

GPO Box 2343
Adelaide SA 5001
Tel (+61 8) 8204 8773
Fax (+61 8) 8204 8777 DX:467
srsaRecordsManagement@sa.gov.au
www.archives.sa.gov.au

State Records of South Australia

Adequate Records Management - Security & Accessibility

Outcome 5: Records are secure and accessible as appropriate

Agencies must ensure that official records are protected from unauthorised or unlawful access, and that measures are in place to prevent loss, damage and destruction. This must be balanced with the need for official records to be readily accessible to authorised persons.

The security of records is essential to ensuring their reliability, integrity and evidential value. It is important that agencies understand the sensitivity of the records they hold, as this is key to correctly identifying the security classifications and measures which should be applied to systems, physical locations and staff members.

The efficient delivery of services is reliant on timely access to records. It is therefore important that agencies balance security requirements against the need for easy and appropriate access to records for business and legislative purposes. Achieving this balance should be the result of a process which defines and documents security and access requirements across the entire agency.

How can my agency meet the requirements of Outcome 5?

Agencies must satisfy a number of requirements to achieve adequacy in relation to Outcome 5 of the *Adequate Records Management (ARM) Standard*:

- Apply government mandated security classifications and access controls to records and staff.
- Implement recordkeeping/business systems and storage facilities that are protected from unauthorised access, intentional illegal destruction or theft, and from damage.
- Make appropriate use of technical security measures including version control and read-only access.
- Provide public access determinations for records transferred to the custody of State Records.
- Document and implement policies and procedures to support records security and accessibility.
- Release information, proactively or via conventional processes, in line with established policies and legislation.
- Assign responsibility for records security and accessibility.
- Gain senior management support for records security and accessibility, which is demonstrated through the provision of secure storage facilities and system controls.

What are the benefits of adequate records security and accessibility?

- Avoid the embarrassment, financial costs and legal implications of unauthorised access to official records.
- Reduction in the costs associated with locating hard to find records.

- Easy access to the records required to deliver agency business, leading to better customer service.
- Minimise the chances for illegal alteration to or illegal disposal of official records.
- Increased confidence in the reliability and evidential value of official records required to support and authenticate the actions and decisions of an agency.

Which government standards apply to records security and accessibility?

State Records has issued the *South Australian Recordkeeping Metadata Standard* (SARKMS) which sets out mandatory metadata elements required to manage records in accordance with best practice. The Standard contains a security classification scheme and access controls applicable to both records and people, which agencies must incorporate in to their recordkeeping programs.

SARKMS should be used by agencies in conjunction with the *Information Security Management Framework* (ISMF), issued by the Office of the Chief Information Officer (OCIO). The ISMF is mandatory for South Australian public authorities. The ISMF sets out policies and standards designed to support the *'security of information stored, processed, transmitted or otherwise manipulated using Information and Communication Technology (ICT)'*[1]. The ISMF identifies technological and physical security measures agencies must adopt to ensure records security.

How do agencies identify and apply access and security requirements?

State Records suggests agencies undertake the following steps to establish and apply access and security requirements.

1. **Undertake a preliminary investigation**. Identify current rules for access and security, including those contained in government and industry-wide legislation, policies, codes of practice and specific regulatory sources. This step may reveal that access and security arrangements should be designed to protect personal and commercially confidential information. Agencies should identify and analyse stakeholders and risk, and determine how these factors may impact on access and security requirements.
2. **Analyse business activity.** Examine business processes and practices in more detail, and identify the records that they generate. This will help agencies understand which records require access and security management and where the risks lie in relation to access and security management.
3. **Analyse current rules.** Closely examine the sources identified in step one and determine what access and security provisions they contain. An assessment of the risks of not meeting these requirements should take place. Agencies should map the requirements to their Business Classification Schemes (BCS)/thesaurus to understand the business context of each requirement.
4. **Make decisions.** Translate the requirements identified in step three to decisions concerning records' accessibility. Agencies should use the access control and classification frameworks outlined in SARKMS and the ISMF to apply these decisions.

[1] Office of the Chief Information Officer, *Information Security Management Framework*, V3.1.1 31 August 2012

5. **Assess existing arrangements.** Examine existing security and access arrangements to determine whether they are able to meet the access and security requirements that have been identified. This will involve assessments of existing policies, systems, and physical storage locations, to determine their capacity to restrict and permit access to records in line with established controls.
6. **Identify and document strategies.** Decide on strategies to help ensure the effective implementation of the access and security program. This is likely to encompass the development of policies, technical components of systems, training programs and business rules.
7. **Implement strategies.** Agencies should now be ready to implement the range of access and security solutions they have developed. Implementation will involve applying access controls and security classifications to records in systems and physical locations, providing staff with the policies and business rules that have been developed, and delivering training to staff.
8. **Undertake a post-implementation review.** Monitor and report on the access and security program regularly, to ensure that it continues to be based on current requirements. Any breaches in security should be reported to senior management and used to inform the monitoring and review process.

Security and access requirements should be defined and implemented across the entire agency. Agencies could however undertake this exercise in stages, focussing on the areas where they have identified higher risks of unauthorised disclosure.

Further information

Adequate Records Management Standard, State Records of South Australia

State Records has produced a number of other Standards, Guidelines and Recordkeeping Information Sheets relevant to security and accessibility aspects of records management. Please refer to the State Records website.

State Records acknowledges use of *DIRKS Manual, Doing a DIRKS Project, Manage Records Access and Security* issued by State Records NSW www.records.nsw.gov.au in the development of this advice.

Version control

Version number	Date of issue	Details
1.0	06/11/2013	First issue

Classification: Public