Australian Capital Territory

Territory Records Office

GUIDELINE

Guideline to Principle 5: Protect Principle

A resource for implementing the Standard for Records, Information and Data

18 August 2016

Table of Contents

INTRODUCTION

Records are evidence of business activity. The *Territory Records Act 2002* (the Act) defines them as 'information created and kept, or received and kept, as evidence and information by a person in accordance with a legal obligation or in the course of conducting business'.

The Act allows the Director of Territory Records to approve standards for records management, which ACT Government organisations must comply with. The ACT Standard for Records, Information and Data was approved in 2016. It sets out seven principles for managing ACT Government records. This Guideline is intended to assist organisations to comply with the Protect principle.

While the term 'record' has a specific meaning, in practice it can at times be difficult to distinguish between records and other types of information or data. Although the Act only applies to records, its principles can be applied to all ACT Government information and data holdings. The Territory Records Office recommends this approach. If there is doubt as to whether ACT Government information or data meet the definition of a record, the standard should be applied.

The Protect Principle

The Protect Principle means ACT Government organisations must secure, store and preserve of records, information and data to protect the interests of the organisation and the rights of employees, clients, stakeholders and citizens, now and into the future.

Organisations must take steps to protect their records, information and data from misuse, interference, loss, unauthorised access, modification and disclosure.

By adhering to the Protect Principle, ACT Government organisations will ensure their records, information and data are managed so they are appropriately protected (secured) for as long as required.

Complying with the Protect Principle

There are two aspects to complying with the Protect Principle:

1. Identifying records, information and data protection requirements: an organisation must ensure it understands its own and the community's requirements to protect records, information and data from inappropriate access, alteration, circulation and destruction.
2. Ensuring appropriate protection measures are in place: organisations must implement measures to protect records, information and data in a range of circumstances including during their storage and handling, outsourcing, digitisation and migration and business continuity planning.

For an organisation undertaking a comprehensive assessment of their records, information and data management, use the Territory Records Office's Compliance Checklist Tool in

association with this and other guidelines to implementing the Standard for Records, Information and Data.

Further information

This guideline should not be read in isolation, as the Standard for Records, Information and Data comprises seven separate but inter-related principles. Each principle is supported by its own guideline.

Along with the seven guidelines, further information can be found in the following resources:

- *Territory Records Act 2002*
- *Freedom of Information Act 1989*
- *Health Records (Privacy and Access) Act 1997*
- *Information Privacy Act 2014*
- International Standard: ISO15489—Records Management part 1
- International Standard: ISO15489—Records Management part 2
- International Standard: 1302—Digitization of Records
- ACT Government Cabinet Handbook
- ACT Government Protective Security Policy Framework
- Territory Records Office *Records Advice* series

IDENTIFYING RECORDS, INFORMATION AND DATA PROTECTION REQUIREMENTS

The process of appraisal, which is described further under the Assess Principle, must analyse an organisation's business activities to determine which records, information and data must be kept to meet the organisation's business needs, accountability requirements and community expectations. This analysis involves understanding the significance of the organisation's activities and the records that result from them, and the risks to the organisation, the community or the government of not having access to reliable records of those activities. As set out in the Assess Principle, assessments of significance and risk must take into account issues of security, privacy, other sensitivities, continuity, accountability and community expectations. These assessments should inform the way records, information and data are created, stored, handled, and accessed.

Security

Organisations must establish measures to ensure records, information and data are maintained in a secure environment, including by determining and controlling who is permitted to access different information and in what circumstances.

The *ACT Government Protective Security Policy Framework* guides the security classification and protection of sensitive ACT Government records, information and data, and should be referenced for full details.

Privacy

The Territory Privacy Principles are outlined in the *Information Privacy Act 2014* and should be referenced for full details. In the context of the public's right to personal privacy, it is important that organisations develop and implement systems and controls to meet privacy requirements.

Other Sensitivities

Organisations should develop and implement guidelines about who is permitted access to records, information and data and in what circumstances.

Access to records may be restricted to protect:

- personal information and privacy;
- intellectual property rights and commercial confidentiality;
- security of property (for example, financial and physical security);
- Territory security; and
- legal and professional privilege.

ACT Government Cabinet information assets must be managed consistent with the ACT Government Cabinet Handbook, which should be referenced for full details. Decisions about access restrictions should also be guided by the Access Principle.

Continuity, accountability and community expectations

As outlined in the Assess Principle, organisations should understand the business needs, accountability requirements and community expectations relating to their records, information and data. Organisations should use the appraisal process outlined in the Assess Principle to determine these requirements and the length of time their records, information and data must be protected from loss, alteration, damage and inappropriate access. This may include identifying vital records, information and data that protect the assets and interests of an organisation, as well as those of its clients and stakeholders, and which may require special management. Records disposal schedules must be produced by the organisation and approved by the Director of Territory Records to identify the period of time for which an organisation's records must be protected to meet business, accountability and community requirements.

ENSURING APPROPRIATE PROTECTION MEASURES ARE IN PLACE

Once an organisations' records, information and data protection needs are known they must be implemented. Records, information and data protection encompasses many aspects including security and access controls, storage and handling, preservation planning, outsourcing controls, digitisation and migration, and business continuity management.

Access controls

Systems managing records, information and data must provide timely and efficient access to the information assets to facilitate ongoing business use and to satisfy accountability requirements.

Systems should apply controls on their access to ensure that the integrity of records, information and data is not compromised. Systems should be configured to provide and maintain audit trails or other mechanisms that demonstrate that records are effectively protected from unauthorised use, alteration or destruction. This may involve controlling or monitoring who is able to view, alter, promulgate or delete records, information and data. The Describe Principle provides further guidance about documenting access to records, information and data.

Managing the access process involves ensuring records, information and data are:

- clearly identified according to their access status at a particular time;
- only released to those who are authorised to see them;
- readable when required and authorised if they are encrypted; and
- used by authorised staff undertaking business process and transactions.

Security and access controls must not be applied over-zealously. Decisions to restrict access to records, information and data must begin from a position of openness, in line with the ACT Government's Open Data policy. Records, information and data should as far as possible be made widely available across the organisation, across the ACT government and to the wider community. The *ACT Government Protective Security Policy Framework* provides guidance on determining when access restrictions may need to be applied to records, information and data.

The monitoring and mapping of user permissions and functional job responsibilities are continuing processes. The Access Principle also provides further guidance on these issues.

Preservation planning

Organisations will likely use many types of systems to conduct their business ranging from human resource systems, finance systems to custom built systems.

Records Management Programs should outline the regime for preserving records and making them accessible over time. This may include the development of an information management plan for each system, which should be appropriately authorised within the organisation. Preservation strategies can include copying, conversion and migration of records, information and data – see the Strategy Principle for further guidance.

Endorsed locations

To be fully accountable, an organisation must know where all its records, information and data are located, and to have access to them. Documentation and location controls should

be applied that enable records, information and data to be identified, retrieved and presented quickly, easily and in a clean state.

Any storage location or facility in which records, information and data are to be held must be endorsed to ensure its appropriate management. Endorsement processes should be outlined as part of an organisation's Records Management Program – see the Strategy Principle for further guidance.

Storage and handling measures

Appropriate storage environments and handling requirements, procedures and systems should be considered when designing systems for records, information and data. This will ensure information assets are protected, accessible and properly managed. The purpose served by the records, information and data, along with their format, use and value, will determine the nature of the storage facility and services required to manage the information assets for as long as required.

Factors that are important in selecting storage and handling options include:

- volume and growth rate;
- usage;
- security and sensitive needs;
- physical characteristics of the records, information and data;
- retrieval requirements;
- relative cost of storage options; and
- access needs.

Care of physical records

The storage environment for physical records must be appropriate to preserve the records for as long as they are required. All physical records, regardless of how long they will be retained, must be stored in premises that have adequate security controls, are protected from pests such as rats and silverfish, and have fire alarms and fire control systems. Storage facilities should not be in locations that have a high risk of fire or flooding.

Records that have been designated as Territory Archives must be kept in higher quality conditions, which should include:

- humidity and temperature controls appropriate for the long term preservation of the records' medium;
- UV filtered lighting;
- heat or smoke detection, fire alarms, sprinkler systems and fire extinguishers;
- adequate security monitoring alarms and controlled access; and
- appropriate housing including shelving and packaging materials.

Unsentenced physical records – that is, those records for which no determination has been made on how long they must be retained – cannot be stored outside ACT Government premises. This also means that unsentenced records must not be stored with commercial

storage providers. Sending to commercial storage physical records whose significance has not been assessed is inefficient and can encourage circumstances where records are retained for longer than they are required. It may also put significant Territory archives at risk. Unsentenced records should be stored with internal storage providers such as ACT Record Services, subject to their policies and requirements.

Physical records that have been identified as Territory archives under an approved records disposal schedule may only be stored outside of ACT Government premises after the organisation has recorded sufficient metadata about the records and provided this metadata to the Territory Records Office. This requirement is intended to ensure that archival records stored outside ACT Government premises are still able to be accessed by the public under the Act. See the Access Principle for further guidance on public access to archives.

The Territory Records Office will specify the metadata required before Territory archives can be transferred outside Territory premises, the format in which it is required, and the frequency with which organisations must report on their Territory archives. This means organisations must ensure they have adequate information about their records before transferring them to commercial storage providers. All ACT government records, information and data that is being transferred to commercial storage providers from 1 January 2017 must have the appropriate metadata recorded by ACT Government organisations, and this information will be reportable to the Territory Records Office. See the Describe Principle for further guidance on metadata requirements for ACT Government records.

More broadly, organisations must have in place arrangements for documenting the location of all of their records. For some organisations insufficient information may have been retained in the past about the location and content of Territory records. In these circumstances, and particularly for those records not stored on Territory premises, organisations should take reasonable steps to properly document recordkeeping metadata and report this to the Territory Records Office, or to return archival records to Territory custody until they can be properly documented.

Care of digital records, information and data

Restrictions on physical storage locations do not apply to digital records, which may be stored in cloud arrangements before they have been appraised according to the Access Principle. Organisations must, however, make careful assessments of their digital records that may be stored and managed in cloud or other off-site arrangements. This includes an assessment of the potential risks to the security, accessibility and reliability of records, information and data, and identification of appropriate mitigation strategies. *Record advices* which outline some of the risks and restrictions of using off-site storage for digital records, information and data are also available. The Territory Records Office can provide further advice regarding assessing and managing cloud arrangements for records, information and data

While there are currently no blanket restrictions on where digital records that are designated Retain as Territory Archives (RTA) may be stored, the Act does oblige

organisations to ensure that Territory archives remain accessible and usable for as long as they are required. Long-term digital storage of records, information and data presents particular problems and will require careful planning for preservation strategies, including for software and hardware migration. These factors should be taken into account in any decision to store digital RTA records outside of Territory-controlled systems or premises.

Outsourced controls

When outsourced providers are engaged to undertake any aspect of ACT Government business, the provider becomes the 'custodian' of ACT Government records, information and data. The ACT Government organisation, however, is ultimately responsible for, and remains the owner of all the records, information and data assets.

These situations require careful planning and specific actions to ensure records, information and data are protected. For example, the contract between the service provider and ACT Government should stipulate that records, information and data will be managed and handled in accordance with the security, privacy, retention and destruction requirements outlined in ACT Government standards, principles and legislation.

Further measures should be taken and planning should be done when outsourcing any aspect of the management of records, information and data. The Director of Territory Records must be informed of the type of arrangement being entered into by the organisation, including physical records storage and cloud-based data or information storage.

Organisations should regularly monitor and review the quality and quantity of records, information and data being created or managed by outsourced providers to ensure the principles outlined in the Standard for Records, Information and Data are being appropriately applied.

Digitisation and migration

When converting a physical information asset (for example, a paper record) to a digital alternative, the process is known as 'digitisation'. Digitisation can be undertaken to either help preserve the original document or to facilitate access.

There are specific issues that must be considered when planning digitisation, including:

- establishing the purpose, planning and justification for digitising, and ensuring appropriate authorisation of digitisation projects;
- considering the right approach to digitisation;
- ensuring correct technical standards are used for digitisation; and
- making correct decisions about managing source records after digitisation—in some cases organisations may still be required to retain hard copy source records even after they have been copied to digital formats.

Migration is the process of moving digital information assets from one software or hardware platform to another. Migration is required for digital records, information and data that are

stored or managed in systems that are being upgraded, superseded or decommissioned. Migration of digital assets requires careful planning and technical expertise, and must be considered early in all decisions relating to business systems that create or keep Territory records, information and data.

Disaster and Business continuity planning

In the event of a disaster, access to records, information, data and associated systems will be required for business to continue. Particular records, information and data assets will be considered essential to re-establishing operations. These are referred to as 'vital' information assets and require special management at all times so they are protected and recoverable when needed. They may include contracts, research data, strategic plans, policy advice, or customer records, payments and receipts.

All organisations should establish plans (and in some cases contribute or be incorporated into organisation-wide planning) for responding appropriately to disasters. Mitigating actions will likely form part of daily operations to mitigate risks associated with disasters occurring, for example, system back-ups.

Organisations must acknowledge and incorporate records, information and data processes to ensure appropriate coverage in the organisations disaster and business continuity plans. Further guidance is available from the Territory Records Office.