Territory Records Office

Records Advice

No. 76

Cloud-based services and recordkeeping considerations

Purpose

This Records Advice has been prepared to provide ACT Government employees with guidelines for understanding recordkeeping requirements when considering using cloud-based or externally hosted services to support ACT government business. This Records Advice should be read in conjunction with Records Advice 77 Cloud-based services and understanding the risks, Records Advice 78 Cloud-based services and mitigating risks, the ACT government's Cloud Policy (TBA) and advice developed by Shared Services ICT.

Background

Cloud computing poses both benefits and risks for ACT government agencies. Efficiency gains and cost savings need to be weighed against the risks that cloud arrangements may present to privacy, security and records management.

For records management, it is essential to consider:

- where records will be stored – there may be risks to ACT government records when they are stored outside Australia.
- the value and nature of the records – higher value records require greater records management control to ensure their integrity, authenticity and reliability.
- the risks that might arise – different cloud services will present different risks to records.
- whether the risks can be satisfactorily mitigated – this may depend on the ability to negotiate contracts and service level agreements.

Agencies are ultimately responsible and accountable for managing their records wherever they are held. Records of value need to:

- retain their integrity, authenticity and reliability;
- be accessible and retrievable; and
- be able to be securely destroyed when authorised, or preserved in perpetuity if they are deemed to be records of archival value.

Legislative context

Legislative requirements need to be adhered to when considering the utilisation of cloud-based services.

The protection of ACT government records is governed by the *Territory Records Act 2002* which requires each agency to ensure the safekeeping and proper preservation of its records and that, when records that are in someone else's possession, they are held under arrangements that provide for the safekeeping, proper preservation and return of the records.

The *Territory Records Act 2002* also requires an agency to advise the Director of Territory Records about any arrangements entered into with an entity that is not an agency to carry out any aspect of its records management. This includes records storage.

The *Territory Records Act 2002* outlines certain protection measures that need to be adhered to by agencies, including:

- not abandoning or disposing of a record; or
- not transferring or offer to transfer, or be a party to arrangements for the transfer of, the possession or ownership of a record; or
- not damaging a record; or
- neglecting a record in a way that causes, or is likely to cause, damage to the record.

Existing notifiable instruments supporting the *Territory Records Act 2002* also impact the utilisation of cloud-based services, including:

The standard for records description and control: records, and the descriptive information about them, must be maintained in an appropriate and secure environment so that they cannot be altered or destroyed without proper approval.

The standard for digital records: records are the responsibility of the agency currently responsible for that function. An agency may delegate or outsource the function, but not the responsibility. Appropriate provisions must be incorporated into agency/provider contracts to ensure outsourced services (including cloud-based service providers) manage the data/records appropriately.

The standard for digital records: agencies must integrate digital recordkeeping requirements into its overall records management program (policies, procedures, responsibilities) including cloud-based services.

The guideline for records management programs: storage and related technologies used for maintaining electronic records can ensure that the evidential elements of electronic records are accessible but cannot be altered. This includes implementing security controls, data administration measures, audit trails and adopting media and open standards that meet longevity and migration requirements.

Other ACT Government legislation, frameworks and policies will also have certain implications, including the Privacy Act and the protective security policy framework.

For more information

See Records Advice 77 Cloud-based services and understanding the risks.

See Records Advice 78 Cloud-based services and mitigating risks.

To view the cloud policy for the ACT government see Cloud Policy (TBA).

Contact the Territory Records Office at:
tro@act.gov.au

Contact Shared Service ICT at:
ICTSharedServices@act.gov.au

The complete list of Records Advices is on the internet at
http://www.territoryrecords.act.gov.au/recordsadvice

More detailed information on the ACT Government records management regime may be found in the Territory Records Office Standards http://www.territoryrecords.act.gov.au/standards and the related Territory Records Office Guidelines http://www.territoryrecords.act.gov.au/guidelines.

This Records Advice was informed by State Records NSW, Public Record Office Victoria, Queensland State Archives and National Archives of Australia.