TAHO
Tasmanian Archive + Heritage Office

# State Records Guideline No 17

# Managing the recordkeeping risks associated with cloud computing

Department of Education
LINC Tasmania

Tasmania
Explore the possibilities

# Table of Contents



### Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

### Document Development History
### Build Status

| Version | Date | Author | Reason | Sections |
|---|---|---|---|---|
| 3.0 | August 2015 | Christine Woods | Template | All |
| 2.0 | February 2014 | Sam Foster-Davies | Revision | All |
| 1.0 | 30-11-2010 | David Benjamin | Initial Release | All |

### Amendments in this Release

| Section Title | Section Number | Amendment Summary |
|---|---|---|
| All | All | |

**Issued:** November 2010

**Ross Latham**
State Archivist

# 1 Introduction

Cloud computing applications are becoming increasingly common. In many cases these solutions may be purchased directly by business units, or even subscribed to by individual users, rather than purchased through formal IT procurement arrangements. Often those acquiring the service may not even be aware they are purchasing a "cloud" service. If a service is marketed using terms such as "bureau", on demand" or "as a service" it is probably a cloud based service.

Cloud computing providers may be located in physical locations which may be beyond state, and even national, boundaries. This raises a number of risks both for government organisations and for members of the public who rely on the proper management of government information to provide evidence of their rights & entitlements, and to demonstrate the workings of government for accountability purposes.

## 1.1 Purpose

This guideline provides information about, and stipulates the process for, the transfer to, or creation of, content in data stores which are maintained by a service provider, remote from the agency. Where government business is done using cloud computing these data stores will contain State records.

## 1.2 Authority

This guideline is issued under the provisions of Section 10A of the *Archives Act 1983*. Guidelines issued by the State Archivist under this Section set standards, policy, and procedures relating to the making and keeping of State records. This section also requires all relevant authorities to take all reasonable steps to comply with these guidelines, and put them into effect.

| **Keyword** | **Interpretation** |
|---|---|
| MUST | The item is mandatory. |
| MUST NOT | Non-use of the item is mandatory. |
| SHOULD | Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing this course. |
| SHOULD NOT | Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course. |
| RECOMMENDS<br>RECOMMENDED | The item is encouraged or suggested. |

'MUST' and 'MUST NOT' statements are highlighted in capitals throughout the Guideline. Agencies deviating from these MUST advise TAHO of the decision to waive particular requirements.

Agencies deviating from a 'SHOULD' or 'SHOULD NOT' statement MUST record:

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- the date at which the decision will be reviewed, and
- whether the deviation has management approval.

Agencies deviating from a 'RECOMMENDS' or 'RECOMMENDED' requirement are encouraged to document the reasons for doing so.

## 2 Identifying the risks

Agencies MUST conduct a thorough risk assessment before entering into any arrangement with a cloud computing service provider. This is particularly important because of the practical difficulties in establishing relationships with global providers and making site inspections of remote facilities when considering commercial arrangements. Further, agencies do not have the capacity to stipulate conditions to consumer service providers such as Facebook, and therefore the responsibility lies with the agency to educate staff as to acceptable use after determining the level of risk.

When conducting a risk assessment, consider the following:

- Does sending or storing information outside of the state or country breach any laws, legislation or standards? (For example few countries have legislation governing the protection & management of personal information).
- Will the records be subject to legislation or other requirements of the storage jurisdiction? (There is a possibility that, if an overseas law enforcement agency subpoenas a cloud computing service provider for access to your organisation's records, you may not be consulted or even notified of this).
- Is there a risk of unauthorised access which may result in breaches to privacy or other laws?
- Is there a risk of a loss of access to records with a subsequent disruption to services?
- Is there a risk of records not being disposed of in a timely way, once authorised by the agency, because it is common for service providers to replicate records for multiple backup. This can mean that time-expired records are not properly deleted from every server held in every site. This can be a serious risk where there is a specific requirement for information to be destroyed, such as personal or sensitive information in records.
- The likelihood of the evidential nature of the records being compromised. If an agency is not able to prove that records could not have been altered in any way, this will negate their value as evidence.
- What are the risks of record destruction or loss due to
    - fire,
    - flood,
    - cyber attack,
    - service provider has gone out of business,
    - the provider claiming ownership of the records,
    - the records not being returned at the conclusion of the contract or returned only on the payment of a large fee;
    - inadequate backup & restoration arrangements as a result of cost saving by the service provider
    - provider may upgrade to hardware or software that is not compatible with the agencies' with the consequent loss of records
    - unlawful disposal

**Assessing risks for different record types.**

Different series of records may carry different levels of risk, depending on their level of sensitivity and importance to the business of an agency. For example:

- records with confidentiality requirements such as prison inmate records, court records and medical records.
- Records that are Commercial-in-Confidence.
- Records of original research

Agencies MUST perform a risk assessment against the information that they are proposing to manage in the cloud. Agencies MUST document this assessment in a risk management plan. You may decide that some records are too sensitive or important to trust to a cloud computing service provider.

**Community expectations**

Community expectations and concerns need to be taken into account. What would the community reaction be to knowing that particular types of information had been sent offshore?

# 3 Selecting a Provider

If after carrying out a risk assessment, your agency decides to engage a cloud computing service provider, you will need to undertake a rigorous selection process to ensure the provider you select can meet your requirements.

- Determine your metadata requirements and ascertain how difficult & costly it will be to make changes to those requirements
- Ascertain the processes around removing your information from the cloud completely, if required, and any costs involved in doing this
- Determine the providers processes around reporting to the agency changes to the jurisdictions in which the information is stored
- Establish if they are they willing to make contractual commitments to comply with privacy requirements on behalf of their clients
- Confirm that an assurance be obtained that no copy of the records or information is retained by the service provider after the termination of the contract
- Verify that the agency is able to regularly specify records to be destroyed and will they provide the agency with certificates of destruction
- Check if they are subject to external auditing or certification processes?
- Determine how third party access to your records be managed, for example, if required by a government watchdog organisation in the jurisdiction in which the records are stored
- Ascertain what back-up arrangement are in place and how long would it take to do a complete restoration of your records if required, and would there be any additional costs for this process? When restoring data can they guarantee that the structure of the records (and not just the content) and associated metadata is maintained.
- Establish if their guaranteed service provision parameters and do they provide recompense if these parameters are not met?
- Determine if they subcontract any part of their services, and if so, under what contractual arrangements do they operate?

# 4 Contractual Arrangements

When entering into commercial arrangements, agencies MUST conduct adequate due diligence on the prospective cloud service provider, their business practices and their security regimes. Agencies MUST use only a cloud service provider that agrees that privacy protection is essential. The contract between the service provider and the government agency MUST:

- ensure that the service provider complies with the Personal Information Protection principles in the *Personal Information Protection Act*;
- set out the procedures that need to be followed in the case of any potential security breach, including notification to the government agency of any breaches, and;
- contain the right for the agency to audit the service provider to ensure it is complying with the *Personal Information Protection Act.*

Agencies MUST ensure that robust contractual arrangements are in place before moving any records to a service provider. A checklist to assist agencies can be found in *TAHO Advice 44 Information Security considerations of Cloud Computing.*

# 5 Monitoring the providers

It is essential that agencies monitor how well your organistion's information management objectives are being met by the cloud computing services used, and check for any unacceptable risks that might emerge.

# 6 A word about Dropbox and other consumer cloud services

There are now a plethora of file sharing and other applications based in the cloud available for consumer use, many at minimal or no cost. Whilst these may appear to offer a quick and convenient way of accessing and distributing information, particularly to a mobile or distributed workforce, agencies are advised to fully investigate the risks and potential business impacts associated with the use of applications such as Dropbox, prior to endorsing for business use.

Items are held in the cloud, in most cases *on servers outside of Australian jurisdiction*, and are therefore vulnerable to scrutiny by law enforcement agencies outside of Australia. Agencies are unlikely to have specific formal agreements in place with the service provider, including documented obligations under Australian law such as the Privacy Act. Utilising external applications such as Dropbox is far less secure than using tools managed in house by agencies for document transfer, and whilst breaches may not be a concern from a loss perspective (as original records should be kept in agency recordkeeping systems), unauthorised access to sensitive information due to security breaches may cause damage to reputation, financial loss, or commercial disadvantage.

Some of the issues to be considered may vary from application to application. Whilst not a prescriptive list, the use of Dropbox in particular should include the following considerations:

- Will you use the standard program or 'Dropbox for Business'?

- Have you read the Dropbox privacy policy (in particular sections 1, 3, 5, 6, and 8)?[1] How does this compare with your agency's own privacy policies, and the agency's obligations under legislation, and specifically the Personal Information Protection Act?
- Have you conducted and documented a full risk assessment before the introduction of Dropbox, and has this been reviewed and endorsed by the agency Executive?
- How will you manage the administration of files added to Dropbox? Who will be responsible for deletion/removal? How will you confirm the 'actual' removal or destruction of files from servers not under your direct control?

These issues are not limited to Dropbox. Examples of other consumer cloud services which allow the storage of information in the cloud include –

- other file sharing apps (eg. Skydrive, Google Drive, etc),
- email applications (eg. Gmail, Yahoo, etc),
- personal storage solutions (eg. iCloud),
- social media (eg. Facebook)

Agencies should advise all staff of the inherent risks of the use of consumer cloud services like Dropbox, and ensure that sensitive information is not included in the usage of such programs. In the event general use is endorsed by the Executive for low risk items, an "approved list" should be included in your 'acceptable use' policy.

# 7 Checklist

| | **Yes** | **No** |
|---|---|---|
| A full & thorough risk assessment has been completed. | | |
| The records you are considering keeping in the cloud are not sensitive, commercial-in-confidence or intellectual property. | | |
| You have taken into consideration community expectations. | | |
| You have undertaken a rigorous selection process for your provider, considering the points raised in this Guideline. | | |
| You have drawn up robust contractual arrangements to cover every foreseeable requirement & eventuality. | | |
| You have in place a process for monitoring how well your information management objectives are being met by the cloud computing services used. | | |

[1] https://www.dropbox.com/privacy

# 8 Definitions

**Agency** - is used in this guideline to refer to all agencies, authorities, statutory offices, departments, councils and other organisations that are subject to, and defined in, the *Archives Act 1983*.

**Cloud computing** – is internet-based computing, whereby shared resources, software and information are provided to computers and other devices on demand. The term 'cloud' is used as a metaphor for the Internet.[2] Cloud computing involves the transfer to or creation of content in data stores which are maintained by the service provider and geographically remote from the customer.

**Record** - is a document or an object that is, or has been, made or kept by reason of any information or matter that it contains or can be obtained from it or by reason of its connection with any event, person, circumstance, or thing. A document includes any printed or written material and an object includes a sound recording, coded storage device, magnetic tape or disc, microfilm, photograph, film, map, plan, or model or painting or other pictorial or graphic work.

**Service level agreement (SLA)** – is a negotiated agreement between two parties where one is the customer and the other the service provider.[3] It records a common understanding about services, priorities, responsibilities & guarantees.

**State records** - are records of State government agencies/departments, State authorities, or local authorities. These public bodies are defined in Section 3 of the *Archives Act 1983*.

.

## Further Advice

For more detailed advice please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

## Acknowledgements

- This guideline is based on a document produced by Australian Digital Recordkeeping Initiative (ADRI), 'Advice on managing the recordkeeping risks associated with cloud computing'.[4]
- and the State Records NSW document 'Managing recordkeeping risk in the cloud'.[5]

[2] http://en.wikipedia.org/wiki/Cloud_computing
[3] http://en.wikipedia.org/wiki/Service_level_agreement
[4] http://www.adri.gov.au/content/products/cloud_computing.aspx
[5] http://futureproof.records.nsw.gov.au/wp-content/uploads/2010/06/Managing-recordkeeping-risk-in-the-cloud.pdf