Public Record Office Victoria
Standards and Policy

Recordkeeping Policy

PUBLIC RECORD OFFICE VICTORIA

Recordkeeping Implications of Cloud Computing

Issue Date: 26/06/2013

Expiry Date: 26/06/2018

PUBLIC RECORD OFFICE VICTORIA

Acronyms

The following acronyms are used throughout this document.

PROV	Public Record Office Victoria
PSPF	Protective Security Policy Framework (For more information see http://www.protectivesecurity.gov.au/Pages/default.aspx)
VERS	Victorian Electronic Records Strategy
ICT	Information and Communication Technology

Copyright Statement

Disclaimer

General

The State of Victoria gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of Victoria shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this Policy. This Policy should not constitute, and should not be read as, a competent legal opinion. Agencies are advised to seek independent legal advice if appropriate.

Records Management Standards Application

The Recordkeeping Standards apply to all records in all formats, media or systems (including business systems). This Policy relates to cloud computing usage by government agencies. Agencies are advised to conduct an independent assessment to determine what other records management requirements apply.

Use of Terminology

The terms ‘record,’ ‘information’ and ‘data’ are used throughout this document. These terms should all be defined as meaning ‘public record’.

Table of Contents

1. Executive Summary: Recordkeeping Implications of Cloud Computing

Cloud computing is a deployment model being employed across the Victorian public sector and in the wider community for the delivery of efficient, flexible ICT solutions and data storage needs. It is expected that the Victorian Government's use of cloud services will continue to expand rapidly and move into new areas in the coming 5 years.

Victorian Government agencies should ensure that any solutions they select are capable of meeting their legal and policy obligations in regards to public records.

Note that this Policy and its supporting Guidelines only address the recordkeeping issues of using cloud solutions. It does not address other issues with using cloud computing.

1.1. Summary of policy

1. When undertaking their risk assessment prior to deploying a cloud solution, agencies should include a specific data risks identification register, with accompanying risk mitigation strategies. Assistance on identifying and managing these risks can be found in the Guidelines that accompany this Policy.

Agencies should particularly consider the implications of storing personal or private information relating to Victorian citizens that carries any security classification[1] (other than "unclassified" under the *Protective Security Policy Framework*) in a cloud that is physically located in a jurisdiction that breaches Victorian privacy or security requirements.

2. Public records should only be stored in a cloud environment capable of complying with all relevant Victorian legislation and policy directives. Assistance on identifying relevant legislation relating to records can be found in the guidelines accompanying this Policy.

Where personal or sensitive data is stored in a public or community cloud, the agency should perform an analysis against the requirements of the *Protective Security Policy Framework*.

3. Agencies should ensure that cloud vendor agreements include sufficient and binding clauses to make certain agency data is effectively protected. A full list of contract clause requirements that relate to recordkeeping is provided in the Guidelines that accompany this Policy.

Agencies should be assured that the service provider is capable of and will execute complete destruction of deleted records.

[1] Please note that the Department of Treasury and Finance *Information Security Policy* requires agencies to implement the PSPF including assigning security classification to their information and monitoring compliance <https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security>

1.2. Suggestions

1. Agencies will find it helpful to categorise the sensitivity of all records to be stored in cloud environments to assist with decision-making as to what portion of the records may be stored in the cloud.

2. Agencies wishing to roll out integrated cloud solutions, incorporating sensitive data as well as less sensitive data, should consider that a private or community cloud offers greater control and certainty, and lower risk, than public clouds.

3. Agencies should consider keeping a secondary (off-cloud) back up of business-critical data, state government vital data and personal / sensitive data to address the risk of loss of data.

Justine Heazlewood

Director and Keeper of Public Records

2. Introduction

2.1. Purpose

Cloud computing is emerging as a central feature of how individuals and organisations use computing resources to create, manage and store information. It is expected that the Victorian government's use of cloud computing, already underway, will continue to expand in line with broader trends worldwide.

This policy gives direction for Victorian government agencies to support best practice recordkeeping when using cloud computing for the purposes of creating, managing, storing, accessing and disposing of public records.

2.2. Scope

This policy applies to all Victorian government agencies bound by the *Public Records Act 1973* and its associated standards. It covers the recordkeeping aspects of decisions made by agencies when using cloud computing in their operations. Agency data stored or created in any cloud are subject to the same PROV records management standards and obligations as Victorian agency data stored in other environments.

2.3. Definition of Cloud Computing

The National Institute of Standards and Technology (NIST), a United States Department of Commerce agency, defines cloud computing as:

"*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction2*".

As the NIST definition is being widely accepted across the Australian government landscape, PROV is accepting this definition as applicable for Victorian government.

It is important to note that this policy is not confined to cloud computing services that can be defined at the time of issue. As the technology evolves, it is expected that many hybrid or novel service models may come into existence. This policy applies to **all** computing services that fit within the NIST definition of cloud computing, regardless of how the services are defined, deployed or limited.

2.4. Related Documents

- Guideline 1: Cloud Computing Decision-Making for Recordkeeping
- Guideline 2: Cloud Computing Tools
- Social Media policy
- PROS 11/10 Access Standard
- PROS 10/13 Disposal Standard
- PROS 11/01 Storage Standard
- PROS 10/10 G6 Records and Risk Management

[2] P Mell & T Grance 2010, *The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Gaithersburg, viewed 18 December 2012,* <*http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*> p. 2.

- PROS 10/10 S1 Strategic Management Specification
- (Forthcoming) Mobile Technologies Policy
- SEC Guideline: Cloud Computing Security Considerations

3. Policy

3.1. Cloud computing decisions should be subject to a data risk assessment

As agencies move more services and data storage into cloud environments, such decisions should ideally be accompanied by a risk assessment that considers the information management risks as a specific issue.

The Victorian Government already mandates that agencies engage in security risk assessment as part of cloud computing decision-making (see Cloud Computing Security Considerations for the Victorian Government). This SEC directive utilises the Victorian Government Risk Management Framework (VGRMF), issued by the Department of Treasury and Finance, which provides for a minimum risk management standard across public sector agencies. Other information management issues can be included in this risk assessment process without creating extra burden on the agency.

The information management risks associated with cloud computing are primarily that:

- Sensitive information (e.g. information about citizens) will be leaked
- Information cannot be retrieved from the cloud supplier and is lost

Thus, when agencies are conducting risk assessment prior to adopting any cloud computing environment, and considering risk mitigation strategies, information management risks should be brought to the fore. The risk assessment may disclose that some data is so sensitive or valuable that it should never be stored in a cloud, while other data (e.g. previously published material, for which inadvertent disclosure is not an issue) may be suitable for a less secured cloud model.[3]

Agencies should consider key risk vectors in their assessment. Areas of common risk, detail on each of these areas, and tools for performing the risk analysis, can be found in the two associated Guidelines to this policy. The *Guideline: Cloud Computing Decision-Making for Recordkeeping* provides a detailed process for assessing each of these areas, while the *Guideline: Cloud Computing Tools* contains a risk matrix template for assessing recordkeeping risks in cloud computing environments.

3.2. Cloud computing use must be capable of compliance with legislation, standards and policies

No agency should store public records in a cloud environment if that cloud environment is not capable of complying with all relevant Victorian legislation and policy directives.

Agencies may find it helpful to complete a legislation and policy requirements review as part of their preparation for cloud computing. The *Guideline: Cloud*

[3] Further information on recordkeeping and risk management is located in *PROS 10/10 G6 Records and Risk Management* <http://prov.vic.gov.au/government/standards-and-policy/all-documents/pros-1010-g6>.

Computing Tools can assist with this process through the *Document Map*, which shows all the generic legislative, standards and policy requirements that bind Victorian agencies. (This Document Map will be updated periodically to remain current with changing regulation.)

However, agencies remain responsible for checking any agency or industry-specific requirements, including specific PROV Retention & Disposal Authorities, which may apply to their cloud computing decision-making.

Furthermore, where personal or sensitive data is to be stored in a public or community cloud, the agency is advised that that an analysis against the requirements of the *Protective Security Policy Framework* (PSPF)[4] is usually appropriate. This analysis will help ensure that such sensitive information is appropriately protected from disclosure.

3.3. Cloud computing agreements must adequately cover data management needs

Agencies should ensure that contracts or service level agreements with cloud computing service providers include sufficient and binding clauses to provide agency data with all the protections it requires. A full list of contract clause requirements that relate to recordkeeping is provided in *Guideline: Cloud Computing Tools (Contract Checklist)*.

Agencies must ensure that contracts or service level agreements with cloud computing service providers clearly identify the agency as the owner of the data, including:

- Affirmation of an agency's ownership of its data, including transactional data created as a result of data being processed on the cloud computing service provider's system, all metadata relating to agency data managed in the cloud, intellectual property rights, and copyright.
- Establishment of the agency as the controller within the contract and determination of the purpose and means of processing data. The cloud service provider's role within the contract should be defined as the processor, processing data on behalf of the controller[5].

END OF DOCUMENT

[4] Australian Government 2013 *Protective Security Policy Framework*, accessed June 2013 <http://www.protectivesecurity.gov.au/Pages/default.aspx>

[5] Dr M Williams 2010, *New Tools for Business, A Quick Start Guide to Cloud Computing, Moving Your Business into the Cloud*