Public Record Office Victoria

Cloud Computing Policy

Guideline 2

Cloud Computing: Tools

Version Number: 1.0

Issue Date: 26/06/2013

Expiry Date: 26/06/2018

Table of Contents

Copyright Statement

Disclaimer

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 Guideline. This Guideline does not constitute, and should not be read as, a competent legal opinion. Agencies are advised to seek independent legal advice if appropriate.

1. Introduction

Victorian Government agencies are increasingly using cloud computing solutions of various kinds for the storage and management of data. This trend is likely to accelerate as cloud computing becomes more cost effective, flexible and responsive over time.

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 interaction1*".

This Guideline is intended to support agencies' moves to using cloud computing solutions. It provides a range of assessment tools which can help isolate key questions and criteria in determining the suitability of proposed solutions for storing and managing public sector data.

1.1. Public Record Office Victoria Standards

Under section 12 of the *Public Records Act 1973*, the Keeper of Public Records ('the Keeper') is responsible for the establishment of Standards for the efficient management of public records and for assisting Victorian government agencies to apply those Standards to records under their control.

Recordkeeping Standards issued by PROV reflect best practice methodology. This includes International Standards issued by the International Organisation for Standardisation (ISO) and Australian Standards (AS) issued by Standards Australia in addition to PROV research into current and future trends.

Heads of government agencies are responsible under section 13b of the *Public Records Act 1973* for carrying out, with the advice and assistance of the Keeper, a programme of efficient management of public records that is in accordance with all Standards issued by the Keeper.

In Victoria, a programme of records management is identified as consisting of the following:

- A recordkeeping framework;
- Recordkeeping procedures, processes and practices;
- Records management systems and structures;
- Personnel and organisational structure; and
- Resources, including sufficient budget and facilities.

A programme of records management will cover all an agency's records in all formats, media and systems, including business systems.

---

[1] 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

As well as its integrated suite of standards, specifications and guidelines, PROV from time to time issues thematic representations of requirements under the heading of Policies. These Policies draw together requirements from several standards as they relate to a particular subject area (eg. Social Media; Cloud Computing). As they derive their authority from the standards, which are mandated instruments of the Public Records Act, Policies are binding on agencies.

Guidelines that link to Policies are created to assist agencies in the practical implementation of the policy requirements, and provide explanation, tools and options for complying with the Policy to which they relate.

1.2. Purpose

The purpose of this Guideline is to facilitate implementation of requirements contained in the *PROV Cloud Computing Policy*. It should be read in conjunction with that Policy and with *Cloud Computing Guideline 1: Cloud Computing Decision-Making*. Guideline 1 provides advice on the areas of assessment included in this tool set.

1.3. Scope

This Guideline applies to the decision-making process for agencies considering or engaging in cloud computing solutions involving the storage and management of data. It covers the relevant questions that agencies will ask to ensure that any cloud computing solution fulfills their data management and storage needs.

It does not cover the due diligence, cost modelling or service efficiency aspects of the decision making process except insofar as they apply to the management of data.

1.4. Structure

This Guideline consists of 4 key structural elements which are designed to be used as tools, either separately or together. Agencies are encouraged to use whichever tools they need for a particular purpose.

For ease of use, the 4 tools are also available as individual files to download in PDF format. The checklists and risk assessment templates are also available as editable Word documents.

The 4 tools provided are:

1. *Risk Assessment Tools*: A risk assessment template, and a. risk matrix, tailored to the cloud computing environment.
2. *Contract Checklist*: A tick-box checklist for use in assessing proposed service contracts in the cloud computing space.
3. *Requirements Checklist*: A template checklist that gathers all PROV requirements together for ease of access.
4. *Document Map*: A visual representation of the intersection of requirements that effect decision making about cloud computing.

1.5. Related Documents

This Guideline should be read and implemented in conjunction with Public Record Office Victoria (PROV) Standards and associated documentation, including appropriate Retention and Disposal Authorities (RDAs). The Policy and other Guidelines directly associated with this Guideline are detailed below.

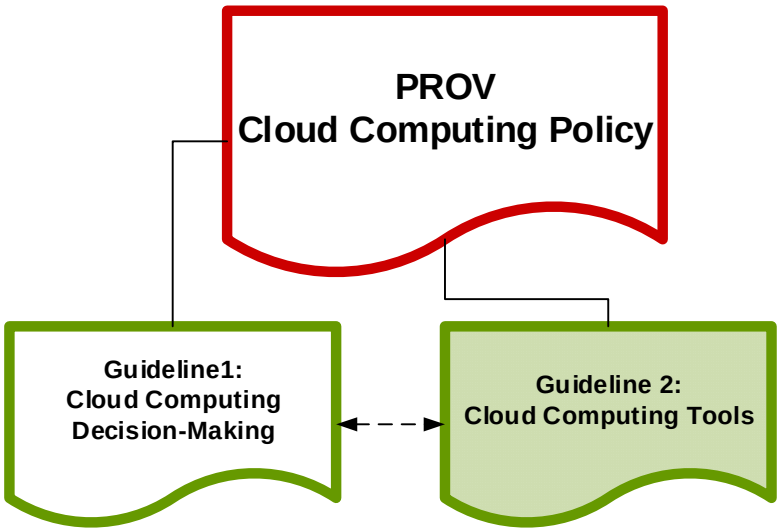


Figure 1: Relationship Diagram

2. Risk assessment

This section contains:

- A risk assessment template, which helps to identify risks in the proposed cloud environment
- A risk matrix, which allows risks to be ranked once they have been identified via the risk assessment template

Agencies may find it useful to start with the risk assessment template[2], using the risk matrix to then assign a level to the identified risks. This will enable the agency to determine where the most significant risks lie.

For an explanation of the risk-based approach to selecting a cloud computing service, please see the *Cloud Computing Policy* (s3.2) and *Cloud Computing Guideline 1: Cloud Computing Decision Making* (s4).

[2] The Department of Treasury and Finance has a Risk Management Framework that is applicable for Victorian government public sector agencies <http://dtf.vic.gov.au/CA25713E0002EF43/pages/economic-and-financial-policy-victorian-risk-management-framework>.

2.1. Risk assessment template

Risk	**Questions**	**Assessment** **1. Describe the cloud's level of service with respect to this risk, including specific contractual terms, audit or test results, and warranties** **2. Based on this information, assign a level to the risk using the assessment matrix above (from Low to Extreme)**	**Mitigation** **1. Outline specific mitigation strategies that will be deployed to reduce the risk** **2. Indicate what level the risk will be at if mitigation is used**
Unauthorised access to sensitive data (ie data with a security classification other than "Unclassified" under the *Protective Security Policy Framework (PSPF)*, OR, if the PSPF is not in use, data that details personal or private information about individuals or contains confidential material of any other kind)	• What protections does the service or environment provide to ensure that there cannot be unauthorised access to data? • What is the track record of the service provider in this regard? (eg have they experienced past security breaches)?		

Risk	Questions	Assessment 1. Describe the cloud's level of service with respect to this risk, including specific contractual terms, audit or test results, and warranties 2. Based on this information, assign a level to the risk using the assessment matrix above (from Low to Extreme)	Mitigation 1. Outline specific mitigation strategies that will be deployed to reduce the risk 2. Indicate what level the risk will be at if mitigation is used
Unauthorised access to or reuse of publicly available data	• What protections does the service or environment provide to ensure that there cannot be unauthorised access to publically available data? (NB: these protections can legitimately be of a lower order than those employed for sensitive data) • How does the service or environment protect data against unauthorised reuse or copying, including data scraping? • What is the track record of the service provider in this regard? (eg have they experienced past security breaches)?		

Risk	Questions	Assessment 1. Describe the cloud's level of service with respect to this risk, including specific contractual terms, audit or test results, and warranties 2. Based on this information, assign a level to the risk using the assessment matrix above (from Low to Extreme)	Mitigation 1. Outline specific mitigation strategies that will be deployed to reduce the risk 2. Indicate what level the risk will be at if mitigation is used

Loss of access to data	• What are the stated service level agreements for access to data:
	  • For normal operations?
	  • For restoration of data after fault or failure?
	• What are the stated service level agreements for:
	  • Time to regain access to data?
	  • Costs involved in regaining access to data?
	• What is the mechanism for protecting data from loss by machine error? (eg mirrors, back-ups)
	• What is the mechanism for protecting data from loss by human agency? (eg errors in processing, inadvertent deletion, intentional or malicious data removal)
	• What is the method by which the return or portability of the data is assured if the service provider goes out of business, changes their service provision, or is no longer the preferred supplier?
	  • In normal circumstances
	  • In abnormal circumstances		

Risk	Questions	Assessment 1. Describe the cloud's level of service with respect to this risk, including specific contractual terms, audit or test results, and warranties 2. Based on this information, assign a level to the risk using the assessment matrix above (from Low to Extreme)	Mitigation 1. Outline specific mitigation strategies that will be deployed to reduce the risk 2. Indicate what level the risk will be at if mitigation is used
Inability to ensure data integrity and authenticity	• What audit and logging facilities does the service or environment provide? • How adequate are these facilities to demonstrate the integrity of data? • How are audit logs provided and made available to clients? • Are logs easily downloadable when moving data off service?		
Inadequate management of data, including metadata	• Can the service retain the required metadata for compliance with PROS 99/007 Specification 2 (VERS Metadata Scheme?)[3] • Can the service demonstrate its capacity to retain and output all metadata required for business purposes?		

[3] http://prov.vic.gov.au/wp-content/uploads/2012/01/VERS_Spec2.pdf

Risk	Questions	Assessment 1. Describe the cloud's level of service with respect to this risk, including specific contractual terms, audit or test results, and warranties 2. Based on this information, assign a level to the risk using the assessment matrix above (from Low to Extreme)	Mitigation 1. Outline specific mitigation strategies that will be deployed to reduce the risk 2. Indicate what level the risk will be at if mitigation is used
Non compliance with Victorian privacy law	• Is it envisaged that the cloud service will be used to store personal and private information about Victorian citizens? • Is the cloud service or any of its storage devices physically located in a jurisdiction with laws that grant powers that, if exercised, would breach Victorian privacy laws? (eg the US due to the Patriot Act) • Is the service operated by an organisation legally registered in a jurisdiction which is under, or can be brought under, laws which breach Victorian privacy law? (eg. US-owned companies operating outside the US will still be vulnerable to the Patriot Act) • What protections does the cloud service have in place to prevent inadvertent disclosure of personal and private data, and to resist forced disclosure?		

Risk	Questions	Assessment 1. Describe the cloud's level of service with respect to this risk, including specific contractual terms, audit or test results, and warranties 2. Based on this information, assign a level to the risk using the assessment matrix above (from Low to Extreme)	Mitigation 1. Outline specific mitigation strategies that will be deployed to reduce the risk 2. Indicate what level the risk will be at if mitigation is used
Non compliance with other Victorian legislation and mandatory policies	• Does the service provider have the capacity to protect the evidentiary integrity of data? • Can the service provider comply with the security requirements imposed by any relevant PSPF assessment? • Can the service provider effectively guarantee the cessation / prevention of data deletion in the case of a legal hold order?		
Non compliance with PROV Standards	• Can the service guarantee data preservation and protection in line with PROV standard requirements? (see Requirements Checklist below)		
Data mining or scraping / copyright protection	• Does the service provider have adequate protections in place to ensure that agency data cannot be mined or scraped by third parties (whether human or automated)? • Does the service provider demonstrate an understanding of the copyright ownership of the data that the agency wishes to store? (NB: Not all agency data will be copyrighted to the state of Victoria, although much will be).		

2.2. Risk Matrix[4]

E – Extreme risk – detailed action plan required
H - High risk – needs senior management attention
M – Medium risk – specify management responsibility
L – Low risk – manage by routine procedures

High or **Extreme** risks must be reported to Senior Management and require detailed treatment plans to reduce the risk to **Low** or **Medium**.

NB: Any one outcome (reputational, business process & systems, compliance or financial) in a Consequence column is sufficient to trigger that level of consequence; there need not be an accumulation of more than one result.

	Consequence				
Reputation	Internal Review	Scrutiny required by internal committees or internal audit to prevent escalation.	Scrutiny required by external committees or Auditor General's Office, or inquest, etc.	Intense public, political and media scrutiny. Eg: front page headlines, TV, etc.	Assembly inquiry or Commission of inquiry or adverse national media.
Business Process & Systems	Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule.	Policy procedural rule occasionally not met or services do not fully meet needs.	One or more key accountability requirements not met. Inconvenient but not client welfare threatening.	Strategies not consistent with Government's agenda. Trends show service is degraded.	Critical system failure, bad policy advice or ongoing non-compliance. Business severely affected.
Compliance	Temporary lapses in complying with advisory or best practice recommendations	Longer term gaps between advisory or best practice positions and service delivery	Temporary and remediable failure to comply with a mandatory policy or legislation	Longer term but remediable failure to comply with a mandatory policy or legislation	Permanent and unremediable lack of compliance with a mandatory policy or legislation
Financial	1% of Budget	2.5% of Budget	> 5% of Budget	> 10% of Budget	>25% of Budget
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
	1	**2**	**3**	**4**	**5**

Likelihood	**Probability:**	**Historical:**							
	>1 in 10	Is expected to occur in most circumstances	**5**	**Almost Certain**	**M**	**H**	**H**	**E**	**E**
	1 in 10 - 100	Will probably occur	**4**	**Likely**	**M**	**M**	**H**	**H**	**E**
	1 in 100 – 1,000	Might occur at some time in the future	**3**	**Possible**	**L**	**M**	**M**	**H**	**E**
	1 in 1,000 – 10,000	Could occur but doubtful	**2**	**Unlikely**	**L**	**M**	**M**	**H**	**H**
	1 in 10,000 – 100,000	May occur but only in exceptional circumstances	**1**	**Rare**	**L**	**L**	**M**	**M**	**H**

Adapted from Standards Australia Risk Management AS/NZS 4360: 2004

[4] Adapted from ACT Insurance Authority, **RISK MANAGEMENT TOOLKIT**, February 2004 (accessed 18/11/12)

3. Data Requirements Checklist: PROV Standards

Please note that the requirements identified in the below tables have been modified to apply specifically to Cloud Computing and are not a direct quote from the relevant Specification.[5]

Standard PROS 11/10: Access **Principle: Access requirements must be capable of being fulfilled with data held within a cloud, in the same way that they would be if the data was stored within the agency.**		
Requirement	**Yes / No**	**Evidence**
Access policies have been documented and communicated to the cloud service provider (Specification 1, 2.1.3)		
Access restrictions are capable of being, and are, enforced within the cloud environment (Specification 1, 2.2.3)		
The security policy that applies to the data has been communicated to the cloud provider and can be fulfilled (Specification 1, 2.5.13, 2.5.15)		
The cloud service is capable of complying with appropriate audit processes (Specification 1, 2.5.16)		

[5] Standards, Specifications and associated documents are available from PROV's website: <http://prov.vic.gov.au/government/standards-and-policy/all-documents>.

Standard PROS 11/07: Capture **Principle: If cloud services are being used to create and capture data, they must be capable of supporting the requirements of authenticity, reliability, useability and integrity.**		
Requirement	**Yes / No**	**Evidence**
The cloud service has been assessed to demonstrate its ability to deliver compliance with data authenticity requirements (Specification 3, 2.2.5)		
The cloud service can capture appropriate change data in a secure way (Specification 3, 2.2.6)		
Data is able to be reliably connected to its required metadata in the cloud environment (Specification 3, 2.3.8)		
Any risks to the preservation of data in the cloud environment have been identified and a mitigation tactic agreed (see risk assessment template) (Specification 3, 2.4.10)		
The cloud service is able to capture and retain both metadata and other associated information required to render the data retrievable, for the entire period in which the data resides in the cloud (Specification 3, 2.4.11 and 2.4.12)		
Any new of special risks of unauthorised access, deletion or alteration of data that resides in the cloud have been identified and mitigated (Specification 3, 2.5.13)		

Standard PROS 10/13 Disposal **Principle: Cloud services must support the legal disposal of data and prevent illegal disposal.**		
Requirement	**Yes / No**	**Evidence**
The cloud service must allow for the imposition of restrictions around disposal of all kinds (Standard, 2.1)		
When data is scheduled for legal destruction, the cloud service must allow this to occur in a complete, timely and secure manner (Standard, 2.7 and 2.8)		

Standard PROS 10/17 Operations Management **Principle: Cloud services must be capable of monitoring, maintenance and adjustment to maximise data outcomes.**		
Requirement	**Yes / No**	**Evidence**
The cloud service must be capable of continuous or periodic monitoring (as the agency determines) to support performance and integrity over time (Specification 1, 2.2.9)		
Data that is to be transferred to another agency or PROV must be capable of being extracted from the cloud environment with all required metadata in a timely fashion (Specification 1, 2.6)		

Standard PROS 11/01 Storage **Principle: If the cloud environment is storing public data, it must be capable of complying with the storage quality requirements imposed on any warehouse used for digital storage. (NB: Agencies are NOT required to restrict cloud providers to those with existing or pending APROSS certification).**		
Requirement	**Yes / No**	**Evidence**
While cloud providers need not be APROSS certified, they should be capable of meeting the minimum standards required of APROSS facilities as outlined in APROSS Guideline (11/01 G1).		

Standard PROS 10/10 Strategic Management **Principle: Decisions to use cloud computing solutions should explicitly consider data and retention requirements in their process.**		
Requirement	**Yes / No**	**Evidence**
Data and records requirements should be explicitly considered and built into the ICT planning for cloud computing. (Specification 1. 2.2.12)		
The contract of service with the cloud provider must build in recordkeeping / data management requirements (see Contract Checklist below) (Specification 1, 2.4)		

4. Contract Checklist

In developing an agreement with a cloud service provider, agencies will need to be mindful of the difficulty of enforcing agreements with organisations based or registered in overseas jurisdictions, in the event of a dispute.

Agencies are reminded that laws regarding data privacy and security differ widely across the world, and that some jurisdictions have additional legal requirements that mean that Victorian law may not be respected with regard to agency data.

For example, data that is stored on servers located within the US, OR with a company that is registered in the US, regardless of where its servers are physically located, is subject to the US Patriot Act, which grants the US security community very widespread powers of data access and surveillance in circumstances which could bring a Victorian agency into breach of privacy law and state security policies.

Agencies are advised to seek independent legal advice.

Requirement	**Yes / No**	**Contract Clause (*Insert number or reference)**
1. Ownership Ownership and custody of data is determined and documented in the legal documents that govern the relationship with contracted service providers. Agencies are reminded that legal and beneficial ownership of data are not always identical at law, and neither necessarily implies custody. For an explanation of the issues to be aware of, see PROS 10/10 Strategic Management Guideline 2: Records of Outsourced Activities <http://prov.vic.gov.au/government/standards-and-policy/all-documents/pros-1010-g2>, (PROS 10/10 s2.4 requirement 21; Guideline 2 recommendation 4.2 Ownership & Custody)		
2. Data management Service providers are required to comply with data management requirements determined by the agency. These requirements should be clearly defined and should incorporate the PROV standards requirements in the checklist above. (PROS 10/10 s2.4 requirement 22)		

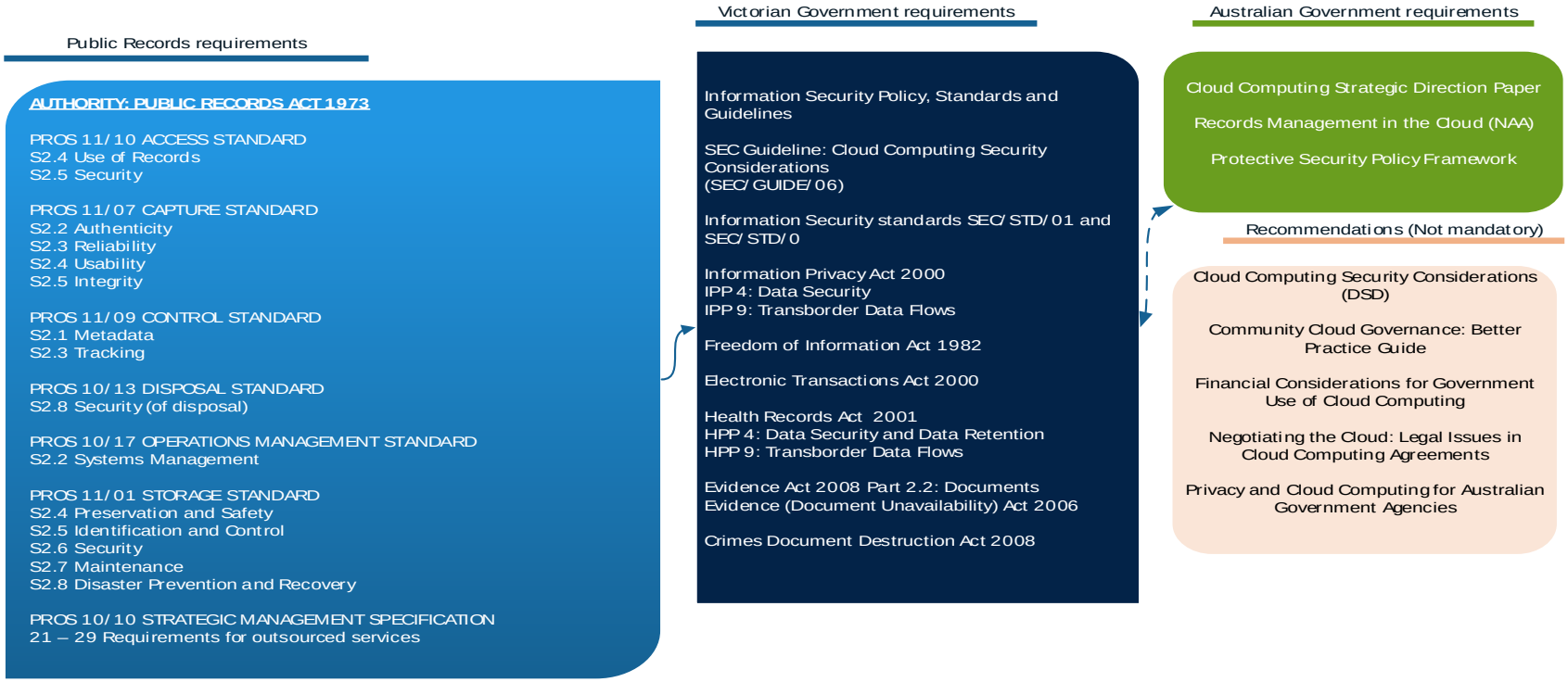
Requirement	Yes / No	Contract Clause (*Insert number or reference)
3. Disposal Contract specifies that records must only be disposed of in accordance with the Public Records Act 1973 and other relevant legislation (PROS 10/10 s2.4 requirement 23)		
4. Access The same level of access to data must be available to the public regardless of who is delivering the service. (PROS 10/10 s2.4 requirement 24)		
5. Storage Appropriate standards of storage with reference to *PROS 99/007 Management of Electronic Records* (VERS Standard) <http://prov.vic.gov.au/government/vers/implementing-vers/standard-2> and *PROS 11/01 Storage Standard* <http://prov.vic.gov.au/government/standards-and-policy/storage> must be included in the contract (PROS 10/10 s2.4 requirement 25)		

Requirement	Yes / No	Contract Clause (*Insert number or reference)
6. Security Appropriate standards of security, based on risk assessment and PSPF assessment, must be mandated in the contract. Specific issues to address are: • Where the service is to be provided from a location within Australia, a prohibition on the provider transmitting data outside of Australia without the prior approval of the agency is appropriate • A requirement for the provider to notify the agency immediately in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively • A requirement for the provider to store data so as to prevent other customers of the provider from accessing the agency's data • The level of security and encryption to be applied to agency data held and transmitted by the provider • the level of access security protocols to be implemented by the provider to defeat unauthorised attempts to access the data • Where physical media is damaged and replaced, requirements for the sanitisation or deletion of data in the damaged media. This should comply with the Protective Security Policy *Information security management guidelines: Protectively marking and handling sensitive and security classified information* (section 10).< http://www.protectivesecurity.gov.au/informationsecurity/Documents/Protectively%20marking%20sensitive%20and%20security%20classified%20information.pdf> A requirement for the provider to destroy or sanitise (or de-identify in the case of personal information) sensitive information held by the provider at the end of the agreement, where such data is not or cannot be returned to the agency. This requirement should specifically include the destruction of all back ups of agency data in the service provider's custody. (PROS 10/10 s2.4 requirement 26		

Requirement	Yes / No	Contract Clause (*Insert number or reference)
7. Audit Arrangements for monitoring and audit of contracted service provider records management practices should be agreed and specified. This may include, as appropriate, agreement terms which act to: • Restrict the locations/countries in which agency data may be held • Grant rights to audit the provider's compliance with the agreement including rights of access to the provider's premises where agency data is being held • Grant audit rights for the agency (or its nominee), the Auditor-General, the Independent Broad Based Anti Corruption Commission (IBAC) <http://www.ibac.vic.gov.au/>, the Keeper of Public Records, the FOI commissioner, the Privacy commissioner and the Health Records Commissioner, and / or any other regulatory body that would have rights to audit the data if it were held locally by the agency • Grant a right for the agency to appoint a commercial auditor as its nominee Where technically available, grants the right for the agency to remotely monitor access to its data and where this is not possible, a requirement that the provider maintain an audit log of access to the agency's data and provide that log to the agency on request. (PROS 10/10 s2.4 requirement 27)		
8. Privacy The service provider must be bound to comply with privacy requirements relevant to the data. This includes: • Explicitly prohibiting the disclosure of personal data to any third party for any reason that would contravene Victorian law • Ensuring that the provider is contractually prohibited from using the data for any of the provider's own purposes such as advertising or other commercial services. (IPP 4: Information Security IPP 9: Transborder Data Flows)		
9. Confidentiality The service provider should be bound to replicate the same level of confidentiality with respect to data that the agency itself must observe.		

Requirement	Yes / No	Contract Clause (*Insert number or reference)
10. Termination and return of data Agreements must include data-specific requirements to be invoked when agreements or relationship end. These include requirements that the service provider: • Give all reasonable assistance in helping with the disengagement and transition including retrieval of all data in formats approved by the agency. As a minimum, the agreement must guarantee that data can be returned in the format provided by the agency. • Supply a detailed disengagement and transition plan to give the agency confidence in the nature and scope of the provider's disengagement services • Not delete any data at the end of the agreement without the express approval of the agency and then implement destruction of all copies when instructed including all back ups • Guarantee effective and timely return of data.		
11. Jurisdiction Agencies should ensure that, at a minimum, the agreement states what country's (and jurisdiction's) laws apply to the agreement, which courts can hear disputes about the agreement (known as the choice of law provisions) and whether alternative dispute resolution mechanisms such as arbitration are proposed. **NB**: Even if carefully drafted choice of law provisions are included in an agreement, it will not necessarily preclude a court from applying different laws where the nominated laws, or forum, are not appropriate in the context of the relevant agreement or dispute.		
12. Remedies in event of breach Aside from any remedies available at law, agencies may wish to include contractual remedies for breaches of aspects of the agreement that involve data. These may include an obligation to go to commercially unusual lengths to restore data that has been lost due to fault of the service provider.		

5. Document Map[6]: Cloud Computing Requirements and Guidelines



[6] Please see the References section for links to the above documents

6. References

Legislation

Crimes (Document Destruction) Act 2005
Electronic Transactions Act 1999
Evidence Act 2008
Evidence (Document Unavailability) Act 2006
Freedom of Information Act 1982
Health Records Act 2001
Information Privacy Act 2000
Public Records Act 1973

All current Victorian legislation is available at http://www.legislation.vic.gov.au

Policies and Guidelines

Public Record Office Victoria (PROV) 2013, *PROV Cloud Computing Guideline 1: Cloud Computing Decision-Making,* PROV North Melbourne, accessed January 2013 <http://prov.vic.gov.au/government/standards-and-policy/policies/cloud-computing>.

Public Record Office Victoria (PROV) 2013, *PROV Cloud Computing Policy,* PROV North Melbourne, accessed January 2013 <http://prov.vic.gov.au/government/standards-and-policy/policies/cloud-computing>.

Standards and Government Requirements

PROV Standards

Public Record Office Victoria (PROV) 2003, *PROS 99/007 Management of Electronic Records*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/vers/implementing-vers/standard-2>.

Public Record Office Victoria (PROV) 2010, *PROS 10/10 Strategic Management Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/strategic-management>.

Public Record Office Victoria (PROV) 2010, *PROS 10/13 Disposal Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/disposal>.

Public Record Office Victoria (PROV) 2010, *PROS 10/17 Operations Management Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/operations-management>.

Public Record Office Victoria (PROV) 2011, *PROS 11/01 Storage Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/storage>.

Public Record Office Victoria (PROV) 2011, *PROS 11/07 Capture Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/capture>.

Public Record Office Victoria (PROV) 2011, *PROS 11/09 Control Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/control>.

Public Record Office Victoria (PROV) 2011, *PROS 11/10 Access Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/access>.

Victorian Government requirements

Department of Human Services (DHS) 2011, *Health and Information Privacy*, DHS Melbourne, accessed January 2013, <http://www.dhs.vic.gov.au/about-the-department/documents-and-resources/policies,-guidelines-and-legislation/health-and-information-privacy-principles>.

Department of Treasury and Finance Chief Information Officers (DTF CIO) 2012, *SEC Guideline: Cloud Computing Security Considerations*, DTF CIO Melbourne, accessed January 2013, <https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security-sec-guideline-cloud-computing-security-considerations>.

Department of Treasury and Finance Government Services Division (DTF GSD) 2012, *Victorian Government Information Security Policy and Guidelines*, DTF GSD Melbourne, accessed January 2013 <http://www.egov.vic.gov.au/policies-and-standards/security-policies-and-standards/victorian-government-information-security-policy-standards-and-guidelines.html>.

Department of Treasury and Finance Chief Information Officers (DTF CIO) 2012, *Information Security Standards SEC/Std/1 and SEC/Std/2*, DTF CIO Melbourne, accessed January 2013, <https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security>.

Department of Treasury and Finance (DTF) 2011 Risk Management Framework, DTF Melbourne, accessed June 2013, <http://dtf.vic.gov.au/CA25713E0002EF43/pages/economic-and-financial-policy-victorian-risk-management-framework>.

Privacy Victoria, Office of the Victorian Privacy Commissioner (PV) 2012, *Information Privacy Principles*, PV Melbourne, accessed January 2013, <http://www.privacy.vic.gov.au/privacy/web2.nsf/pages/information-privacy-principles>.

Australian government requirements and recommendations

Australian Government (AG) 2011, *Protective Security Policy Framework: Information security management guidelines: Protectively marking and handling sensitive and security classified information*, AG Canberra, accessed January 2013, <http://www.protectivesecurity.gov.au/informationsecurity/Documents/Protectively%20marking%20sensitive%20and%20security%20classified%20information.pdf>.

Australian Government Information Management Office (AGIMO) 2012, *Community Cloud Governance: Better Practice Guideline*, AGIMO Canberra, accessed January 2013 <http://agimo.gov.au/policy-guides-procurement/cloud/>.

Australian Government Information Management Office (AGIMO) 2012, *Financial Considerations for Government Use of Cloud Computing*, AGIMO Canberra, accessed January 2013 <http://agimo.gov.au/policy-guides-procurement/cloud/>.

Australian Government Information Management Office (AGIMO) 2012, *Negotiating the Cloud: Legal Issues in Cloud Computing*, AGIMO Canberra, accessed January 2013 <http://agimo.gov.au/policy-guides-procurement/cloud/>.

Australian Government Information Management Office (AGIMO) 2012, *Privacy and Cloud Computing for Australian Government Agencies*, AGIMO Canberra, accessed January 2013 <http://agimo.gov.au/policy-guides-procurement/cloud/>.

National Archives of Australia (NAA) 2012 *Records Management and the Cloud*, NAA Canberra, accessed January 2013 <http://www.naa.gov.au/records-management/agency/secure-and-store/rm-and-the-cloud/index.aspx>.

Other Resources

ACT Insurance Authority (ACTIA) 2004, *Risk Management Toolkit*, ACTIA, accessed November 2012, <http://www.treasury.act.gov.au/actia/RM.htm>.

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

For more information about Cloud Computing and public sector data, please contact:

Standards & Policy Team
Public Record Office Victoria
Ph: (03) 9348 5600
Fax: (03) 9348 5656
Email: agency.queries@prov.vic.gov.au
Web: www.prov.vic.gov.au