Public Record Office Victoria

Recordkeeping Policy
Recordkeeping and cloud services

Version number: 1.0
Issue Date: 19 June 2024
Expiry Date: 19 June 2029

1. Application

The Keeper of Public Records has approved this recordkeeping policy for recordkeeping and cloud services. Public offices should apply its terms in line with the *PROV Value and Risk Policy*[1] to relevant recordkeeping decisions and practices, and the *PROV Managing Records in Business Systems Policy*[2] and *PROV Data and Recordkeeping Policy*[3] for recordkeeping obligations around systems and data.

2. Policy

This policy gives direction for Victorian government agencies to support compliance with the mandatory PROV Standards when using externally provided technologies / infrastructure ("cloud services").[4] Records (including data and information)[5] created and captured under cloud service arrangements remain public records and it is the responsibility of the public office to ensure they are managed in compliance with PROV Standards. This means:

1. Any cloud services that support public records use or process[6] must be capable of compliance with the mandatory requirements detailed in PROV Standards and Specifications.[7]
2. All cloud service arrangements should be subject to a value and risk-based approach to resourcing and implementing records management programs[8] (alongside any information security value assessments) [9], including defining and establishing:
    a. Any recordkeeping requirements in contractual arrangements with service providers.[10]
    b. Monitoring performance against the recordkeeping requirements, as part of contract management, this includes:

---

[1] *PROV Recordkeeping Policy: A value and risk-based approach to records management*, available via PROV's website.

[2] *PROV Recordkeeping Policy: Managing Records in Business Systems Policy*.

[3] *PROV Recordkeeping Policy: Data and Recordkeeping Policy*.

[4] An external provider is an autonomous entity engaged to deliver a service, distinct from the governmental agency or department engaging their services. Also known as a third-party provider, these external entities provide a range of services such as consulting, software development, and outsourcing. A third-party provider may encompass services provided by another agency or department.

[5] See PROV Data and Recordkeeping Policy for further definition.

[6] Agencies must also consider effective management of transactional data within cloud services, including its transfer and migration (where applicable). This encompasses implementing robust systems for data organisation, access control, retention policies, and security measures to safeguard sensitive information and facilitate efficient recordkeeping practices.

[7] See PROV *Standards framework*.

[8] See PROV Value and Risk Policy and topic page on High value, high risk records.

[9] See OVIC Information security resources.

[10] *PROS 24/01 Operational Management Standard* states that "Agreements for contracting services, programs or products for a public office or on behalf of a public office specify requirements for recordkeeping" (Principle 6). This principle applies regardless of who is providing the contracted services.

i. That the service is accessible and available to those that manage and have authorised use for the service.
ii. That the service can be managed effectively, including:
- Maintaining the evidential value[11] to ensure the preservation of authentic, complete, and meaningful records.[12]
- Establishing mechanisms and processes to ensure integrity from unauthorised modification.
- That the service protects the privacy and security of the information in line with relevant Victorian legislative requirements.[13]

3. That the service can facilitate agencies to meet retention and disposal obligations under the *Public Records Act 1973*[14] and in accordance with the Recordkeeping Standards issued by the Keeper of Public Records under the *Act*, ensuring:
   a. The application of relevant and current Retention and Disposal Authorities to public records.
   b. Public records (including data /information) are securely managed until they can be lawfully and securely disposed of.
   c. Long term temporary and permanent value digital records are kept in a long-term secure and sustainable format.[15]
4. Agencies must retain control and ownership of public records when engaging cloud services to mitigate risk to public records.[16] This includes:
   a. Assessments to identify the governing jurisdiction for:
      i. Hosting arrangements to safeguard that data is held in accordance with legislative requirements.[17]
      ii. Foreign-owned company arrangements. Noting that these can be subject to foreign legislative, regulatory or administrative obligations, regardless of where the data is held, that could jeopardise the security and accessibility of public records.
   b. Prioritising redundancy planning for both storage and backup solutions, aiming to ensure uninterrupted access to public records.[18]
5. Using an external provider must not reduce the accessibility and availability of the records for an agency or the public, including:
   a. Ensuring authorised staff within agencies maintain access[19] to fulfil obligations in line with Freedom of Information (FOI) applications, inquiries, royal commissions or other legal obligations.[20]
   b. Implementing preservation strategies to guarantee that public records can be opened, accessed, and read beyond the confines of the cloud service, ensuring their ongoing accessibility and readability.[21]
   c. When an agreement ceases with a service provider, arrangements are made to continue management of public records by the agency, ensuring continued access to securely manage the records until they can be transferred or lawfully destroyed.

---

[11] This corresponds with the definition of a public record as outlined in the *Public Records Act 1973*, referencing the *Evidence Act 2008*, and further reinforced by the *Crimes Act 1958* regarding the preservation of records for legal proceedings, including the explicit handling of evidence destruction.

[12] In line with *PROS 19/05 Create, Capture and Control Standard* Principle 2 it is expected that "Records must be preserved for the period of time they must be retained". This is inclusive of all formats and extends to systems managed by external providers but remains the responsibility of the public office.

[13] See PROV Legislation topic page for more information.

[14] See *Public Records Act 1973* and *PROS 22/04 Disposal Standard*.

[15] See *PROS 19/05 S3 Long Term Sustainable Formats*.

[16] Control involves the obligation to securely maintain public records, ensuring their authenticity and reliability. Controls should be designed in such a way to ensure records remain credible evidence, generated through consistent procedures, with clear origins, and safeguard against damage or alteration for the retention requirements of the records See also PROS 19/05 Create, Capture and Control Standard.

[17] Consideration needs to be given to Principle 9—Transborder Data Flows of the Information Privacy Principles.

[18] See PROV Recordkeeping Policy: Backup Technologies and Records Management.

[19] Under the *Freedom of Information Act 1982*, having access to or ownership of the records is referred to as "possession".

[20] See Freedom of Information Act 1982 and OVIC FOI resources for agencies for further clarification.

[21] See PROV *Cloud services and computing* and *Microsoft 365* topic pages for considerations around preservation of cloud services.

3. Background

PROV developed this policy to address the need for agencies to manage public records in accordance with PROV Standards, irrespective of whether they are created, captured and managed by in-house or externally provided technologies and infrastructure.

Cloud services involve providing computing resources—like servers, storage, databases, networking, software, and more—over the internet. Instead of owning and managing physical hardware or software, users can access these resources on-demand from cloud service providers. Cloud services offer scalability, flexibility, and cost-effectiveness since users can pay for what they use without the need for extensive infrastructure investments. Cloud services can encompass Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), among others.

Agencies engaging cloud service providers must uphold robust accountability mechanisms. The *Public Records Act 1973* stipulates that heads of Victorian public offices bear the responsibility of establishing and upholding recordkeeping programs. They must allocate adequate resources and delegate responsibilities effectively to ensure streamlined record management across the organisation. This includes meticulous contract management procedures, ensuring adherence to PROV Standards. Furthermore, agencies must maintain continuous oversight of public records creation, capture, control, access, and disposal throughout the contractual process and ongoing provider management. Comprehensive planning processes is supported by the *PROS 24/01 Operational Management Standard*, which outlines mandatory requirements, supplemented by guidance provided in the *Operational Management Standard Implementation Guide*.[22] Additionally, VPS organisations have obligations for managing contracted service providers under the Privacy and Data Protection Act 2014 (section 88(2)).[23]

Ensuring the accessibility, security, and longevity of records stored within cloud services necessitates a comprehensive assessment of an agency's ability to maintain its public records in the event of service unavailability, including when arrangements cease. The integration of M365 operations with cloud services is a recognisable example. Should access to such services become compromised, it not only jeopardises the retrieval of vital records but also impairs the functionality crucial for effective agency operations. Therefore, careful planning, secure backup strategies, and ensuring redundancies are imperative to help manage the risks associated with potential service disruptions and safeguard the confidentiality, integrity, and availability of public records. Implementing redundancies can involve maintaining alternate backup systems, regularly testing these backups, and having alternative access solutions in place. This ensures that even in the face of primary service failure, critical records remain accessible and agency operations continue uninterrupted.

4. Appendix

Backup Technologies and Records Management Policy, PROV 2024 (https://prov.vic.gov.au/recordkeeping-government/document-library/backup-technologies-policy-backup-technologies-and)

Data and Recordkeeping Policy, PROV 2024 (https://prov.vic.gov.au/recordkeeping-government/document-library/data-policy-data-and-recordkeeping-policy)

Information Management Requirements for Software-as-a-Service, CAARA 2020 (https://www.caara.org.au/wp-content/uploads/2020/07/Information-Management-Requirements-for-Software-as-a-Service-V1.0-May-2020.pdf)

Managing Records in Business Systems Policy, PROV 2023 (https://prov.vic.gov.au/recordkeeping-government/document-library/business-systems-policy)

[22] See PROV Procurement - sourcing and contract management topic page for more information.

[23] See Privacy and Data Protection Act 2014 and OVIC Resources for organisations for further clarification.

Procurement - sourcing and contract management Topic Page, PROV 2023 (https://prov.vic.gov.au/recordkeeping-government/procurement-sourcing-and-contract-management).

Record Keeping Assessment Tool (RKAT) (https://prov.vic.gov.au/recordkeeping-government/learning-resources-tools/rkat)

Standards Framework Topic Page, PROV 2023 (https://prov.vic.gov.au/recordkeeping-government/standards-framework)

Value and Risk Policy, PROV 2022 (https://prov.vic.gov.au/recordkeeping-government/document-library/value-risk-policy)

VEO creation, PROV 2023 (https://prov.vic.gov.au/recordkeeping-government/a-z-topics/veo-creation)

Victorian Protective Data Security Framework (VPDSF), OVIC 2023 (https://ovic.vic.gov.au/information-security/framework-vpdsf/)

Victorian Protective Data Security Standards (VPDSS), OVIC 2019 (https://ovic.vic.gov.au/information-security/standards/)

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 Standard.