

Public Record Office Victoria

Recordkeeping Policy Enterprise Mobility

Version number: 1.0
Issue Date: 03 December 2024
Expiry Date: 03 December 2029

1. Application

The Keeper of Public Records has approved a recordkeeping policy for **enterprise mobility**.¹ Public offices should apply the policy's terms in line with the following when using mobile devices,² applications, and technologies that facilitate remote access to records (including data and information) for business purposes:

- the Recordkeeping Standards,³ including retention and disposal authorities⁴
- the *PROV Value and Risk Policy*⁵
- the *PROV Recordkeeping and Cloud Service Policy*⁶
- the *Managing Records in Business Systems Policy*⁷
- the *Data and Recordkeeping Policy*.⁸

2. Policy

It is Public Record Office Victoria's (PROV) position that:

1. **Full and accurate records of the business of the office must be created, captured, managed, and disposed of lawfully and in line with the Public Records Act⁹ regardless of the location, service, or device used.**
 - a. Records remain related to the context of the business that they were created for and used within.
 - b. Records are captured and stored in line with the records management processes and business rules of the office for the duration of their retention periods.
 - c. Records are disposed of lawfully.

¹ Enterprise Mobility relates to situations in which personnel work can work anywhere and anytime due to a combination of mobile devices, applications, and technologies that facilitate remote access to data. Mobile devices include both Internet-enabled and Internet-capable devices (such as smart phones, tablets, laptops, handheld gaming devices and digital cameras) and non-Internet portable devices (such as handheld sound recorders, portable storage items, and non-digital photographic equipment). Devices, applications, and technologies used may be owned by the business or be personally owned.

² Mobile device includes personal devices or services used for business purposes.

³ <https://prov.vic.gov.au/recordkeeping-government/standards-framework>

⁴ <https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas>

⁵ <https://prov.vic.gov.au/recordkeeping-government/document-library/value-risk-policy>

⁶ <https://prov.vic.gov.au/recordkeeping-government/document-library/cloud-services-policy-cloud-services-policy>

⁷ <https://prov.vic.gov.au/recordkeeping-government/document-library/business-systems-policy>

⁸ <https://prov.vic.gov.au/recordkeeping-government/document-library/data-policy-data-and-recordkeeping-policy>

⁹ Including the PROV Standards and Retention and Disposal Authorities (RDAs) issued under section 12 of the *Public Records Act 1973*.

2. **Responsibility for recordkeeping¹⁰ is clearly documented, expressed, understood, and demonstrated, regardless of the location, service, or device used.**
 - a. Ultimate responsibility remains with the head of a public office in line with the *Public Records Act 1973*.
 - b. Responsibility for overall management is delegated by the head of a public office to appropriately knowledgeable and skilled personnel.
 - c. General responsibility is assigned to all personnel.
 - d. Contracts and agreements include recordkeeping, where appropriate.
3. **Governance¹¹ covering mobile devices, applications, and technologies that facilitate remote access to data, include and address recordkeeping in line with legislative requirements,¹² business needs and community expectations. Governance should include the following:**
 - a. Compliance with PROV Standards, Specifications, and Retention and Disposal Authorities throughout
 - i. the lifecycle of the device, application, and technologies that facilitate remote access to data
 - ii. the retention period of the records.
 - b. Compliance with other state and sector wide law, security, information, identity, access, privacy, and data management requirements when creating, accessing or managing records.
 - c. Requirements for managing business records that are held on personal devices.
 - d. Service, app, and device requirements; including boundaries (such as what apps can be downloaded, how business records are accessed), virus protection, patching protocols, system basics, syncing, device management, and remote access to the device by the public office IT staff, if needed.
 - e. Education for staff using the service, device, apps, or technologies regarding their responsibilities as public officers to create and keep full and accurate records of the business of their office.
 - f. Technical issues where a decision point is required to help manage record security or maintenance, such as whether files will be auto synced, or what kind of technical support (if any) corporate IT will provide.
4. **Risks to the records must be identified, documented, assessed and mitigated regardless of the location, service or device used.**
 - a. Security risks are identified and mitigated using the Victorian Protective Data Security Framework (VPDSF) assessment process¹³ and in line with relevant cyber security strategies.¹⁴
 - b. Risks to the authenticity and integrity of the records are identified and mitigated, including risk related to data quality, intellectual property, and ownership/control of data.
 - c. Preservation risks are identified and mitigated in line with the Victorian Electronic Records Strategy, PROV Standards (including Retention and Disposal Authorities), and business continuity plans.
 - d. Privacy Impact Assessments¹⁵ are used to identify and mitigate privacy, identity, and access risks.

3. Background

Enterprise mobility refers to remote access to records across a range of scenarios both in the office and externally. For example, an employee may hot desk when in the office. They may need to access, create and capture office records when travelling between the office and an external location or when working from home. Certain places may be declared off-limits through policy or other means, due to the increased risk of sensitive records being leaked. For example, when on a train or in a café as an unauthorised person may read over your shoulder, intercept and steal personal information (such as passwords), and may even hack into your computer through publicly available Wi-Fi vulnerabilities.

¹⁰ Please note that under the Public Records Act 1973, the definition of record includes information and data.

¹¹ Governance includes business rules, policies and processes.

¹² Legislative requirements include PROV recordkeeping standards, associated specifications, and retention and disposal authorities.

¹³ <https://ovic.vic.gov.au/>

¹⁴ <https://www.cyber.gov.au/>

¹⁵ <https://ovic.vic.gov.au/>

A program of records management undertaken in an environment where records are being accessed remotely must address the challenges and complexities of the services, devices, apps and technologies used. For example, hot desking in an office environment may focus on addressing risks associated with cloud environments¹⁶ and third-party providers¹⁷, including intellectual property management, maintaining evidential value, and ensuring access to records for the duration of their retention periods. Working on a personal mobile device outside of an office environment may have additional focus areas around determining what are personal and what are business records, movement of records between the personal device and the office environment, and removing or deleting records and associated metadata.

PROV developed this policy to ensure that public records are appropriately and lawfully created, captured, managed and disposed of, regardless of the location, device, or service used. Under the *Public Records Act*, a public record is “any record made or received by a public officer in the course of the officer's duties”. Section 13 of the Act requires that the Head of a Public Office “cause to be made and kept full and accurate records of the business of the office” in accordance with PROV Standards and disposal authorities. The Act is technologically neutral and does not specify the formats or technologies needed to create, capture or manage records. The location a public officer needs to be in when creating, capturing or managing records is not mentioned either. Where specific formats, technologies or location specific information is required, it will be addressed in PROV’s Standards and Policies.

Identifying and managing risk to records is an essential part of a records management program. This includes managing risk to the integrity, authenticity, reliability, and usability of the records, addressing privacy and security risks,¹⁸ and ensuring that lawful disposal actions are carried out. Records must be managed for the duration of their retention periods, which are often longer than the lifespan of specific systems, services, technologies, devices, and apps. Methods for maintaining records over time may need to include migration and conversion strategies, especially if records are required to be preserved as State Archives and transferred to PROV once business needs have concluded.

Copyright Statement

© State of Victoria 2024



Except for any logos, emblems, and trademarks, this work is licensed under a Creative Commons Attribution 4.0 International license, to the extent that it is protected by copyright. Authorship of this work must be attributed to the Public Record Office Victoria. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/legalcode>

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.

¹⁶ For more information on managing cloud services, please see our topic page: <https://prov.vic.gov.au/recordkeeping-government/a-z-topics/cloud-services>

¹⁷ For more information on procurement and contract management, please see our topic page: <https://prov.vic.gov.au/recordkeeping-government/procurement-sourcing-and-contract-management>

¹⁸ For more information on privacy and security, please refer to the Office of the Victorian Information Commissioner: <https://ovic.vic.gov.au/>