Public Record Office Victoria

GUIDELINE

Managing Records in M365

Version number: 1.0
Issue Date: 01 July 2022
Expiry Date: 01 July 2027

This guideline covers the following areas to assist with management of records in Microsoft 365:

- Design and configuration of M365 implementations
- M365 licences, contracts, or agreements
- M365 systems governance structures
- Creation and capture of records of business conducted in M365
- Access to records in M365
- Contextual relationships between records in M365
- Monitoring M365 for risk to records
- Disposal of records in M365
- Migrating records from within M365 to external systems
- Decommissioning M365
- Transferring permanent value records from within M365 to PROV

Table of Contents

Public Record Office Victoria Standards 4

Purpose and Scope 4

About the CAARA Issued Functional Requirements 4

M365 and Recordkeeping 6

Using this Guideline 7

1 Design and Configuration 8

1.1 General Implementation advice 8

1.2 Corresponding Requirements in PROV Standards 9

2 Licenses, Contracts and Agreements 11

2.1 General Implementation Advice 11

2.1 Corresponding Requirements in PROV Standards 12

3 Governance Structures 13

3.1 General Implementation Advice 13

3.2 Corresponding Requirements in PROV Standards 14

4 Creation and Capture 16

4.1 General Implementation Advice 16

4.2 Corresponding Requirements in PROV Standards 17

5 Access Management 18

5.1 General Implementation Advice 18

5.2 Corresponding Requirements in PROV Standards 19

6 Contextual Relationships 21

6.1 General Implementation Advice 21

6.1 Corresponding Requirements in PROV Standards 22

7 Risk Management 23

7.2 General Implementation Advice 24

7.1 Corresponding Requirements in PROV Standards 24

8 Disposal 27

8.1 General Implementation Advice 28

8.1 Corresponding Requirements in PROV Standards 28

9 Migration 30

9.1 General Implementation Advice 30

9.1 Corresponding Requirements in PROV Standards 31

10 Decommissioning 33

10.1 General Implementation Advice 33

10.1 Corresponding Requirements in PROV Standards 33

11 Transfer of Permanent Records 35

11.1 General Implementation Advice 35
11.1 Corresponding Requirements in PROV Standards 35

12 Useful Resources 37

12.1 Office of the Victorian Information Commissioner 37
12.2 Risk Management Framework 37
12.3 Information Management Framework 37
12.4 Council of Australasian Archives and Records Authorities 37

13 Glossary of Terms 38

Introduction

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 public offices to apply those Standards to records under their control.

Heads of public offices are responsible under section 13b of the *Public Records Act 1973* for carrying out a program of efficient management of public records. The program of records management needs to cover all records created by the public office, in all formats, media and systems, including organisational systems.

It is mandatory for all Victorian public offices to follow the principles and comply with the requirements of the Standards issued by the Keeper.

Purpose and Scope

This guideline is based on the Council of Australasian Archival and Recordkeeping Authorities (CAARA) issued paper *Functional Requirements for Managing Records in Microsoft 365*[1] (hereafter referred to as the CAARA M365 Paper).

Please note that it repeats multiple sections from the CAARA M365 Paper for ease of reference. Additional content strives to align the CAARA principles and requirements with PROV Standards to assist agencies with implementation in the Victorian jurisdiction. Agencies must keep accurate and reliable information about their decisions, actions, and agreements regarding M365 in line with PROV Standards.

This guideline applies to any system holding records, or other information assets, that uses M365 as a core component. It also applies to records and information regardless of whether they are required to be retained short-term, long-term, or permanently.

About the CAARA Issued Functional Requirements

CAARA comprises the heads of the government archival authorities of the Commonwealth of Australia, New Zealand and each of the Australian States and Territories. The main aim of CAARA is to collaborate, share knowledge and resources to improve records and archival management across Australasia. To achieve this aim, CAARA oversees several working groups, including the Australasian Digital Recordkeeping Initiative (ADRI).

The CAARA M365 Paper was developed by an ADRI working group consisting of representatives from the various Australasian records and archival authorities, led by PROV. The purpose of setting up the working group was to have a consistent set of requirements for records in M365 that would address records and information management needs of government agencies across Australasia. This was in recognition that public sector agencies are increasingly using M365 to create and manage their records.

The CAARA M365 Paper was issued in October 2021 after several years of development by the ADRI working group. The paper included a set of 11 principles and 47 requirements, as well as some general guidance on their application.

[1] https://www.caara.org.au/wp-content/uploads/2021/12/Functional-Requirements-for-M365-Version-1.0.pdf

Audience

The CAARA M365 Paper was developed for service providers, implementers, and agency personnel involved in the specification, procurement, project management, or maintenance of systems using M365 as a core component. This includes government agency personnel or contractors working on behalf of a government agency who:

- control or manage records and information
- develop, implement, or maintain systems that control or manage records and information
- develop and oversee contracts or agreements that involve the services or systems that control or manage records and information.

Assumptions/prerequisites

The CAARA M365 Paper assumes that the agency has an established records and / or information management framework in place based on recordkeeping best practice. For the Victorian jurisdiction, this means in line with the Standards issued by the Keeper, as well as other legislative and regulatory obligations, business needs and community expectations.

The strategies and mechanisms included in the framework ensure that:

- authority and responsibility for the appropriate management of information in systems, including information assets, are formally assigned, and delegated to people with the relevant skills and knowledge
- assigned owners are aware of their responsibilities regarding managing the information assets assigned to them
- full and accurate records of agency business are routinely and reliably captured into authorised systems by all personnel (including contractors and volunteers).

The CAARA M365 paper also assumes that good recordkeeping practices (including authenticity, reliability, and integrity controls) are included in the design for all areas of the agency, as well as for all systems, processes, and policies. This includes ensuring that system specifications address metadata elements needed to support business needs and maintain trustworthy records (for example, metadata supports record identification, useability, accessibility, and context).

The creation and maintenance of the documentation outlined in the table below is strongly recommended:

Action undertaken by	**Description of action required**
Agency	Document the recordkeeping requirements, including those specific to the agency and those required by legislation/regulation
Implementer	Document how and where the requirements are met in the system
Agency	Document the authorisation / sign-off specifying that the requirements are met
Agency / Service Provider	Maintain 'as built' documentation of the recordkeeping model

M365 and Recordkeeping

M365 is intended to be customised to whatever you want or need it to be. To deliver the well-defined functions of a recordkeeping or specialised business system, M365 must be configured appropriately, and relevant technical and management controls put into place. M365 is fully hosted and maintained in Microsoft's Azure Cloud and is therefore an 'evergreen' system in that Microsoft will continue to upgrade and make changes to the products and their components. These changes will be implemented on Microsoft's schedule, which is regular and frequent. Agencies should be aware of the changes and actively monitor how changes may impact integration with other systems and business-specific configurations of M365.

Implementations of M365 are based on a license structure that has a variety of different tiers, each of which has slightly different components, applications, and capabilities. This guideline does not specify whether a specific licence of M365 is required or whether an external product should be used. The individual agency decides whether to implement these requirements natively or via a third-party product.

Please note:

M365 will be used throughout this guideline and is interchangeable with other similar Microsoft product suites including Office 365 and SharePoint Online.

System will be used throughout to mean systems based on M365. The system in this context includes any additional Microsoft or third-party add-ins and organisational processes.

Agency will be used throughout to mean an organisation that is subject to *Public Records Act 1973*.

Agencies must make and keep full and accurate records of business activity, appropriate to their business processes, regulatory environment, and risk and accountability requirements in accordance with PROV Standards.[2] The agency must determine:

- the records that are needed
- how the records should be described (i.e., required metadata)
- how the records should be created (i.e., responsibilities and processes)
- how these records are to be consistently and routinely captured (i.e., systems, processes, formats).

This determination must be based on the value and function of the records to the organisation, government, and the community, considering both current and future needs.[3]

A record can be formally created and managed, like a legal casefile; or they can be ad hoc, like notes from a phone call. They also include all work information that is collected using a personal device, like a mobile phone. A full and accurate record comprises:

- record content
- record metadata
- any system metadata that supports its trustworthiness.

[2] https://prov.vic.gov.au/recordkeeping-government/standards-framework

[3] For guidance on determining value, see the PROS 19/03 G - Strategic Management Guideline (https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-g-strategic-management-guideline)

Trustworthy records have the following characteristics, which are actively maintained for as long as the record exists:

- **Authenticity**: The record is what it claims to be, including who created or sent it and when.
- **Reliability**: The contents of the record can be trusted as a full and accurate representation of the facts. The contents of the record can be depended upon by the agency, the government, and the community, and relied upon in legal proceedings.
- **Integrity:** The record is complete and unaltered. Any authorised additions or annotations are explicitly indicated and traceable.
- **Useability:** The record can be located, retrieved, and presented in a timely manner. It should be linked to any related records.

In line with PROV Standards, agencies must ensure that records and other information assets are linked to business functions and objectives (using metadata). Agencies are required to analyse and document the information that must be created and managed across the organisation applicable to the regulatory environment in which they operate. This does not need to be a formal Business Classification Scheme but must be functionally equivalent. Agencies should include records and information related risk in their risk management programs.

Using this Guideline

For ease of use, this Guideline is divided into eleven sections plus appendices, with each section based on a principle from the CAARA M365 Paper and its underlying requirements.

Each section includes a table of correspondences with PROV Standards, as well as guidance specific to that principle from the CAARA M365 Paper. Additional resources for the Victorian jurisdiction are in an appendix at the end of this Guideline.

Please note that the correspondences should be used as **a starting point only** as an agency's records management program will extend beyond their M365 implementation. A PROV principle or requirement may only be partially addressed by fulfilling a CAARA principle or requirement, and more than one PROV requirement may be applicable when addressing a CAARA principle or requirement.

It is expected that the agency will determine how their specific regulatory and legislative requirements and business needs align with their M365 implementation. To that end, the agency must do a full value and risk analysis to determine what their specific record and information management requirements are and how their M365 implementation and ongoing maintenance will address those requirements. This includes how their implementation will meet PROV Standards.

All PROV Standards and associated Specifications and Guidelines mentioned in this Guideline are available via the PROV Standards Framework Topic Page: https://prov.vic.gov.au/recordkeeping-government/standards-framework

1 Design and Configuration

Principle 1:	Design and configuration of M365 implementations must include recordkeeping requirements

REQUIREMENTS	
R1.	The use of persistent metadata for records must be supported. • The system should, as far as possible, support its routine capture (including automation where this is possible). • If the system is not able to ensure that persistent metadata is supported, the record must be moved to a system that can support it.
R2.	Systems holding records must enable them to be identified, retrieved, and used for the period of time they must be retained.
R3.	The system must prevent the unauthorised or premature destruction of records (including contextual metadata).
R4.	The system must protect metadata from unauthorised deletion or modification. The system should allow an authorised records or system administrator to alter the metadata of a record if required, such as, to allow finalisation or correction of the record profile. Any such action must be captured as additional records management metadata.
R5.	The system must support the design and implementation of protection and security controls to ensure records are only accessed, amended, used, released, or disposed of as authorised. Access, security, and user permissions for systems managing records and information must be documented and implemented.

1.1 General Implementation advice

When developing strategies and plans for the design and configuration of M365, consider how the following can be clearly defined:

- the systems authorised to capture and manage records
- the configurations required within those systems to ensure that records are lawfully and effectively managed
- the metadata elements required to ensure records and information are persistent and remain accessible and useable for as long as they are required. This includes metadata required for records and information to:
    - retain contextual identity
    - be identifiable and locatable as required
    - retain integrity as evidence of business
    - address legislative and regulatory requirements
- methods to ensure M365 systems and applications are searchable so records and information are locatable, retrievable, and useable as required
- mechanisms to enable records and information to be identifiable, locatable, retrievable, trustworthy, and useable as required.

Key metadata stored in log files should be copied to a place where it can continue to be associated with the record for the duration of the record's retention period. This is to protect it from deletion as log files do not generally retain metadata in association with the record.

Key metadata should also be protected from unauthorised alteration, especially metadata that is subject to unintended alteration by folder movement or other actions (for example, date / time metadata which often is changed when a record or folder is moved).

The system should maintain a log containing the history of all changes in the order of occurrence and ensure that the system does not overwrite the historical log.

Where the system lacks the functionality or controls to prevent the unauthorised or premature destruction of records, alternative methods will need to be put in place to ensure that records are not placed at risk. For example, it may be necessary to move the records to an alternate location that can prevent their premature destruction.

1.2 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 1	**PROS 19/04 Operational Management Standard** Principle 1 System Planning and Procurement and associated requirements	**PROS 19/03 Strategic Management Standard** also feeds into this work. An assessment of the agency's records management program against the principles and requirements of **PROS 19/03** and how they would relate to the M365 work would be a prerequisite.
Requirement 1	**PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture and associated requirements **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirements 2 and 3, and **PROS 19/05 S2 Minimum Metadata Requirements Specification**	If the M365 will include permanent as well as temporary, or long-term temporary records, the metadata elements required for **PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** may also apply. If the records need to be moved, then **PROS 19/04 Operational Management Standard** Principle 2 System Maintenance, especially Requirement 2, should also be considered. **PROS 19/05 Create, Capture and Control Standard** Principle 3 Controls will also be required to ensure that the transition of records to another system does not reduce their credibility and trustworthiness as evidence.
Requirement 2	**PROS 19/06 Access Standard** Principle 3 Accessibility and associated requirements **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirements 1 and 4 and where necessary **PROS 19/05 S3 Long Term Sustainable Formats Specification** **PROS 20/02 Storage Standard** Principle 3 Survival as Readable records	This also links in with metadata[4] requirements as per **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve (especially Requirements 2 and 3) **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** Also required is a clear understanding of what records need to be kept, what is needed for them to be full and accurate so they can be easily identified, and how long they need to be kept for.
Requirement 3	**PROS 19/06 Access Standard** Principle 3 Accessibility and associated	This requires the relevant **retention and disposal authorities** to be known and implemented in the system to ensure that minimum

[4] Information on **metadata** is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/metadata

	requirements **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control, especially requirement 2 **PROS 20/02 Storage Standard** Principle 2 Protection and Security **PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation	retention periods are set, and appropriate measures put in place to ensure the disposal sentences are carried out appropriately[5]
Requirement 4	**PROS 19/05 Create, Capture and Control Standard** Principle 3 Control, especially requirement 2 **PROS 20/02 Storage Standard** Principle 2 Protection and Security **PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation	This also links in with metadata requirements as per **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirements 2 and 3. **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** Also required is a clear understanding of what records need to be kept, what is metadata is needed for them to be full and accurate, what an authorised adjustment or disposal of metadata associated with a record would look like, and how long records and their associated metadata need to be kept for.
Requirement 5	**PROS 19/04 Operational Management** Principle 2 System Maintenance, especially requirement 2 **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially requirement 2, and principle 3 Control and associated requirements. **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 20/02 Storage Standard** Principle 2 Protection and Security	Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[6] Also required is an understanding of protection and security from a whole of agency perspective, with alignment of strategy, governance, and assessment/measurement structures across relevant areas. See **PROS 19/03 Strategic Management Standard**.

[5] Information on **Disposal** and **RDAs** is located here: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas

[6] See Section 12.1 for useful links.

2 Licenses, Contracts and Agreements

Principle 2:	M365 licences, contracts or agreements must not place records at risk

REQUIREMENTS	
R6.	When contracting a provider to deliver services, programs, or products to the agency or on behalf of the agency, recordkeeping requirements must be identified and included in contracts and agreements.
R7.	The agency must identify and exclude records that are unsuitable for management in a public cloud (Software as a Service (SAAS)) system.
R8.	Risks to applications and systems due to cloud hosting, contracting, outsourcing, or service level agreement must be identified, documented, and mitigated; or if the risk is accepted, then justification is provided.

2.1 General Implementation Advice

In most jurisdictions, records are not public records if they result from business conducted by contractors unless this is specified in contracts and agreements. However, work undertaken by contractors on behalf of agencies is considered the responsibility of the agency, which means that the agency is held responsible for any breach of law or regulation that results.

It is therefore important to consider how contracts and service level agreements can be best used to minimise risk of loss, unauthorised alteration, deletion, or access to records and information within M365.

It is recommended to review the requirements of the *ADRI Information Management Requirements for Software-as-a-Service*[7] and address any areas of risk as appropriate.

Also recommended is to identify and document requirements that are to be put in place to protect high value / high risk records from being placed at risk. This includes any types of records that must be excluded from the systems to protect them.

Data sovereignty must be maintained by ensuring that high value / high risk records are processed, stored, and maintained within Australia.

[7] https://www.caara.org.au/wp-content/uploads/2020/07/Information-Management-Requirements-for-Software-as-a-Service-V1.0-May-2020.pdf

2.1 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 2	**PROS 19/04 Operational Management** Principle 1 System Planning and Procurement and Principle 5 Contracting, especially requirement 1 **PROS 20/02 Storage Standard** Principle 4 Risk Management and Principle 5 Use of External Storage Providers	**PROS 19/04 G Operational Management Guideline** includes information about contracts and agreements in relation to records management, including contract clauses for recordkeeping. The CAARA Paper on **Information Management Requirements for Software-as-a-Service** provides additional guidance regarding potential risks to records
Requirement 6	**PROS 19/04 Operational Management** Principle 5 Contracting, especially requirement 1 **PROS 20/02 Storage Standard** Principle 4 Risk Management and Principle 5 Use of External Storage Providers	**PROS 19/04 G Operational Management Guideline** includes information about system and recordkeeping requirements, as well as contracts and agreements in relation to records management, including contract clauses for recordkeeping. An assessment of what records the agency needs to create, capture, and manage, what is needed for full and accurate records, how long they need to be managed for, and any special considerations (such as format, access requirements and so on) will feed into this work.
Requirement 7	**PROS 19/04 Operational Management** Principle 5 Contracting **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control, especially requirement 2 **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 2 Protection and Security, Principle 3 Survival as Readable Records, and Principle 4 Risk Management	**PROS 19/03 G Strategic Management Guideline** includes information on identifying risk to records and identifying the value of records. Areas of risk to consider include preservation risks, security risks, and risks to maintaining the integrity of the records as credible and trustworthy evidence. **PROS 19/04 G Operational Management Guideline** includes information about contracts and agreements in relation to records management, including contract clauses for recordkeeping.
Requirement 8	**PROS 19/04 Operational Management** Principle 5 Contracting, especially requirement 1 **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control, especially requirement 2 **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 2 Protection and Security, Principle 4 Risk Management, and Principle 5 Use of External Storage Providers	**PROS 19/03 G Strategic Management Guideline** includes information on identifying risk to records, as well as on identifying the value of records. Areas of risk to consider include preservation risks, security risks, and risks to maintaining the integrity of the records as credible and trustworthy evidence. Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[8] **PROS 19/04 G Operational Management Guideline** includes information about contracts and agreements in relation to records management, including contract clauses for recordkeeping.

[8] See Section 12.1 for links.

3 Governance Structures

Principle 3: M365 systems must have effective governance structures in place

REQUIREMENTS	
R9.	Documentation of systems design and configuration must be maintained and kept up to date. The documentation must describe how the system has been configured to meet requirements for managing records. Change decisions must be documented and 'as built' documentation updated.
R10.	Records and information held across diverse system environments or physical locations must be identified and documented.
R11.	The implementation of any third-party applications, or system changes such as upgrades, component replacement, migration, and changes to service or hosting arrangements must ensure that the records are protected and remain accessible for as long as lawfully required.
R12.	Documentation must be maintained to show that records and information management requirements are assessed in system acquisition, system maintenance and decommissioning. Modifications are implemented where required.
R13.	Maintenance must be resourced and routinely undertaken to ensure that systems which hold records are reliable and operate effectively.

3.1 General Implementation Advice

Control mechanisms for the ongoing governance of M365 and associated systems should be in place and actively managed by people with appropriate skills and authority. Control mechanisms include:

- monitoring updates to the product and the associated modifications required to maintain configuration settings, system integration needs, and the agency's business needs
- maintaining the appropriate skills and knowledge, levels of technical and information management personnel to ensure they have the appropriate competencies to manage records held and maintained within M365
- managing the balance between records management requirements, user needs, and technical capacity to ensure that the system continues to support records management.

3.2 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 3	**PROS 19/04 Operational Management** Standard Principle 2 System Maintenance	**PROS 19/03 Strategic Management Standard** feeds into this work. **PROS 19/03 G Strategic Management Guideline** provides guidance on recordkeeping governance and strategic planning. **PROS 19/04 G Operational Management Guideline** includes information about system and recordkeeping requirements, which would need to be considered when developing and implementing governance structures.
Requirement 9	**PROS 19/06 Access Standard** Principle 3 Accessibility, especially requirement 2 **PROS 20/02 Storage Standard** Principle 1 Authorisation and Principle 4 Risk Management	**PROS 19/04 G Operational Management Guideline** sections on systems planning and procurement, and system maintenance, can help with flagging what may need to be documented. This may also link in with metadata requirements as per **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirements 2 and 3; **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** **PROS 19/03 Strategic Management Standard** and associated Guideline include sections on establishment, accountability and responsibility which links into this work. They also contain information on assessment and measurement, which relies on appropriate documentation to do well.
Requirement 10	**PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture **PROS 19/06 Access Standard** Principle 3 Accessibility, especially requirement 1 **PROS 20/02 Storage Standard** Principle 1 Authorisation and Principle 4 Risk Management	This may also link in with metadata requirements as per **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirements 2 and 3; **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** **PROS 19/04 G Operational Management Guideline** sections on systems planning and procurement, and system maintenance, provides some guidance on recordkeeping requirements and functionality that may help with determining what records will need to be held in what systems.
Requirement 11	**PROS 19/04 Operational Management** Principle 2 System Maintenance, especially requirement 2, and Principle 5 Contracting, especially requirement 1 **PROS 19/05 Create, Capture and Control**	**PROS 19/04 G Operational Management Guideline** sections on system maintenance includes some things to look out for when transitioning between systems.[9] This requires the relevant **retention and disposal authorities**[10] to be known and implemented in the system to ensure that minimum

[9] For additional information, see also PROV's **Migration** Topic Page: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/migration and **Decommissioning** Topic Page: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/decommissioning

[10] Information on **RDAs** is located here: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas

	Standard Principle 2 Preserve, especially requirement 2	retention periods are known. Retention periods are set according to the function the record relates to and vary from a matter of days to the lifetime of a person or beyond (for example, if the record is permanently required). This means that some records will need to be kept beyond the lifespan of the system. Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[11]
Requirement 12	**PROS 19/04 Operational Management** Principle 1 System Planning and Procurement and Principle 2 System Maintenance **PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture **PROS 19/06 Access Standard** Principle 3 Accessibility, **PROS 20/02 Storage Standard** Principle 1 Authorisation and Principle 3 Survival as Readable Records	**PROS 19/04 G Operational Management Guideline** sections on systems planning and procurement, and system maintenance, can help with flagging what may need to be documented. This may also link in with metadata[12] requirements as per **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirements 2 and 3; **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** Assessment and measurement are addressed in **PROS 19/03 G Strategic Management Guideline.**
Requirement 13	**PROS 19/04 Operational Management** Principle 2 System Maintenance **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 2 Protection and Security, and Principle 3 Survival as Readable Records	Refer to the **PROS 19/04 G Operational Management Guideline** section system maintenance for additional information.[13]

[11] See Section 12.1 for links.

[12] Information on **metadata** is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/metadata

[13] General information about **M365 and recordkeeping** is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/microsoft-365

4 Creation and Capture

Principle 4:	Records of business conducted in M365 must be created and captured

REQUIREMENTS	
R14.	Any reuse of a record's content as part of a business transaction must result in the creation of a new record in a new context. The new record must include independent metadata about its point of capture and management processes.
R15.	Records created or captured as part of collaborative work involving third parties must be managed to not risk the integrity of the record.

4.1 General Implementation Advice

Agencies must keep accurate and reliable information about their decisions, actions, and agreements.

A Public Record is any information created, maintained, sent, or received by government officers whilst carrying out their work. All information, regardless of format, that is created or received by an agency should be regarded as a public record. PROV should be consulted for any exceptions.

Public records can be created in a range of formats, including hardcopy and digital. They might include:

- emails
- online chats
- messages, such as SMS or other messaging systems, whether encrypted or otherwise
- Microsoft Teams meetings
- Microsoft Power BI software product data
- minutes from meetings, online or face-to-face
- recordings of meetings
- posts on social media
- authorisations given via a system workflow
- information / data within a database.

Records and information created, captured, and imported into M365 systems should:

- include sufficient contextual details to ensure that they are full and accurate
- remain readable and accessible for the duration that they are required
- retain their integrity as evidence
- be locatable and retrievable as required.

4.2 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 4	**PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture **PROS 19/04 Operational Management Standard** Principle 3 Processes	Information about identifying records that can be managed as a group is in the **PROS 19/03 G Strategic Management Guideline**.[14] **PROS 19/04 G Operational Management Guideline** includes information about building creation and capture of records into processes within systems.
Requirement 14	**PROS 19/04 Operational Management Standard** Principle 3 Processes **PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture **PROS 19/06 Access Standard** Principle 3 Accessibility,	This may also link in with metadata[15] requirements as per **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirements 2 and 3; **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification**
Requirement 15	**PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially requirement 3, and Principle 3 Control, especially requirement 1	**PROS 19/04 G Operational Management Guideline** includes information about contracts and agreements in relation to records management, including contract clauses for recordkeeping. The CAARA Paper on **Information Management Requirements for Software-as-a-Service**[16] provides additional guidance regarding potential risks to records. An assessment of what records the agency needs to create, capture, and manage, what is needed for full and accurate records, how long they need to be managed for, and any special considerations (such as format, access requirements and so on) will feed into this work.

[14] General information about **where to start** regarding managing records is located here: https://prov.vic.gov.au/recordkeeping-government/getting-started

Information on **how long records should be kept** is located here: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept

[15] Information on **metadata** is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/metadata

[16] https://www.caara.org.au/wp-content/uploads/2020/07/Information-Management-Requirements-for-Software-as-a-Service-V1.0-May-2020.pdf

5 Access Management

Principle 5:	**Access to records in M365 must be proactively managed from creation and capture to disposal**

REQUIREMENTS	
R16.	Imported records must preserve the integrity of the record (content and metadata).
R17.	All records must be maintained in a format that is expected to survive and remain accessible and readable using readily available software for the required life of the record.
R18.	Bulk retrieval of content and metadata for secondary use in unrelated applications must be allowed
R19.	All information, including information created, accessed, or modified by contractors and third-party providers engaged in outsourcing arrangements, must be accessible when required. The agency must ensure that the records are not put at risk if the service provider is acquired by another organisation during the contract, and that records are returned to the agency at the end of contract, including relevant metadata, in the form the agency specifies.
R20.	The system must support the implementation of security classifications and requirements that are applicable to the sensitivity of the information. Records that carry security classifications (i.e., those requiring an elevated level of protection) must be handled and stored in compliance with the requirements of the classification.

5.1 General Implementation Advice

Information and records captured or stored anywhere within the M365 environment should remain protected and accessible by authorised people for the duration of their retention periods and in accordance with security and privacy requirements. Agencies should store information securely and appropriately to ensure it remains accessible for as long as required. Information should remain accessible for as long as needed and is shared as necessary (subject to access, security, and privacy rules) within a protected and trusted environment.

To ensure that all records are maintained in a format that is expected to survive and remain accessible and readable using readily available software for the required life of the record, training will be required, and actions ma y need to be done manually.

Access to records and information within M365 systems should be proactively managed from creation and capture to disposal. This includes:

- authentication processes and mechanisms to ensure access to records and information only those authorised
- system configurations and business rules covering user rights to clarify what users can access and to what degree
- governance plans and data policies addressing restrictions to access as well as the consequences of inappropriate access
- where protective markings are used, the system configurations, processes, and mechanisms ensure protective markings on records are applied and managed as required

- processes and mechanisms to ensure continued and appropriate access to records and information for the duration of their retention periods regardless of whether they remain within the M365 environment or are exported to another system
- where automation is possible, the system identifies a record on creation, applies the correct classifications and controls to the record (including the correct retention period and disposal sentence), associates the record with the relevant metadata set, and reports on the creation to those who manage records for validation and authorised adjustments where needed.

5.2 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 5	**PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture	**PROS 19/04 G Operational Management Guideline** includes information on system and process requirements that feed into this work. This may also link in with metadata[17] requirements as per **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirements 2 and 3; **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** The relevant **retention and disposal authorities**[18] will need to be known to ensure that any special additional considerations, such as format or the need to migrate the record between systems[19], for example, can be applied.
Requirement 16	**PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially requirements 2 and 3, and Principle 3 Control, especially requirement 1	**PROS 19/04 G Operational Management Guideline** includes information on system and process requirements, including transition, that feed into this work. This may also link in with metadata requirements located within **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** Assessment and measurement are addressed in **PROS 19/03 G Strategic Management Guideline** and may be of value for this work. Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[20]
Requirement 17	**PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture, and Principle 2	**PROS 19/05 S2 Long Term Sustainable Formats Specification** for formats required for permanent and recommended for long term

[17] Information on **metadata** is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/metadata

[18] Information on **RDAs** is located here: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas

[19] Information on **migration** is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/migration

[20] See Section 12.1 for links

	Preserve **PROS 19/06 Access Standard** Principle 3 Accessibility, especially requirement 2 **PROS 20/02 Storage Standard** Principle 2 Protection and Security, especially requirement 2, and Principle 3 Survival as Readable Records, especially requirement 1	temporary records. The retention period will need to be known to determine the best format to retain the record and preserve its integrity over time.
Requirement 18	**PROS 19/06 Access Standard** Principle 3 Accessibility, especially requirement 2	**PROS 19/04 G Operational Management Guideline** includes information on system and process requirements, including transition, that feed into this work. This may also link in with metadata requirements located within **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification.**
Requirement 19	**PROS 19/04 Operational Management Standard** Principle 2 System Maintenance, especially requirement 2 **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve **PROS 19/06 Access Standard** Principle 3 Accessibility, especially requirement 1 **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 2 Protection and Security, Principle 3 Survival as Readable Records, and Principle 4 Risk Management **PROS 22/04 Disposal Standard** Principle 2 Implementation	**PROS 19/04 G Operational Management Guideline** includes information about system and recordkeeping requirements, as well as contracts and agreements in relation to records management, including contract clauses for recordkeeping. **PROS 19/03 G Strategic Management Guideline** includes information on identifying risk to records and identifying the value of records. The CAARA Paper on **Information Management Requirements for Software-as-a-Service**[21] provides additional guidance regarding potential risks to records.
Requirement 20	**PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 20/02 Storage Standard** Principle 2 Protection and Security, and Principle 3 Survival as Readable Records	Information on system security is included in **PROS 19/04 G Operational Management Guideline.** This may also link in with metadata requirements located within **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** The CAARA Paper on **Information Management Requirements for Software-as-a-Service** covers privacy and security in relation to software-as-a-service systems.

[21] https://www.caara.org.au/wp-content/uploads/2020/07/Information-Management-Requirements-for-Software-as-a-Service-V1.0-May-2020.pdf

6 Contextual Relationships

Principle 6: Contextual relationships between records in M365 must be maintained

REQUIREMENTS	
21.	A minimum set of required metadata must be associated with a record at the time it is created or captured by the agency to establish its authenticity, reliability, integrity, and useability over time. This metadata must remain with the record when it is exported or migrated. The minimum metadata requirements are set by jurisdictional, legal, business requirements, and community expectations.
22.	Wherever possible and practical, metadata should relate a record to other records in the system (for example, in a grouping or aggregation), other systems, and other entities.
23.	Metadata regarding the events, actions, and decisions that are relevant to the record must be captured (for example, in some cases it is necessary to log who has viewed the record). This includes the capture of changes to access controls as metadata.

6.1 General Implementation Advice

Groupings are used, for example, to apply rules to a group, to perform operations on a group, to group objects as a composite record. Email is a record and must be managed as such. Emails that provide evidence of business activities should be stored with other related records and be defined with similar metadata. This may require emails to be copied to a different system.

Relationships between records and information in M365 and associated systems should be appropriately described to enable their accurate and efficient identification and timely retrieval. This includes system configurations, policies, processes, and mechanisms that:

- connect records and information relating to the same body of work
- assign version and authorisation controls
- connect records and information within M365 with related records and information held externally, including physical records
- describe actions that have been taken.

The system must be able to retain relational metadata for as long as the record is required. If it is not, other ways of preserving contextual metadata along with the record may be needed.

6.1 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 6	**PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve and Principle 3 Control **PROS 19/05 S2 Minimum Metadata Requirements Specification**; for permanent records - **PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** **PROS 19/06 Access Standard** Principle 3 Accessibility	**PROS 19/04 Operational Management Standard** for system requirements that would support the collection, validation, and use of contextual metadata. Also refer to in **PROS 19/04 G Operational Management Guideline.** The CAARA Paper on **Information Management Requirements for Software-as-a-Service**[22] covers metadata in relation to software-as-a-service systems.
Requirement 21	**PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture, Principle 2 Preserve and Principle 3 Control **PROS 19/05 S2 Minimum Metadata Requirements Specification**; for permanent records - **PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** **PROS 19/06 Access Standard** Principle 3 Accessibility	Refer to **PROS 19/04 Operational Management Standard, PROS 19/04 G Operational Management Guideline** and the CAARA Paper on **Information Management Requirements for Software-as-a-Service.**
Requirement 22	**PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture, Principle 2 Preserve and Principle 3 Control **PROS 19/05 S2 Minimum Metadata Requirements Specification**; for permanent records - **PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** **PROS 19/06 Access Standard** Principle 3 Accessibility	Refer to **PROS 19/04 Operational Management Standard, PROS 19/04 G Operational Management Guideline** and the CAARA Paper on **Information Management Requirements for Software-as-a-Service.**
Requirement 23	**PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture, Principle 2 Preserve and Principle 3 Control **PROS 19/05 S2 Minimum Metadata Requirements Specification**; for permanent records - **PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** **PROS 19/06 Access Standard** Principle 3 Accessibility	Refer to **PROS 19/04 Operational Management Standard, PROS 19/04 G Operational Management Guideline** and the CAARA Paper on **Information Management Requirements for Software-as-a-Service.** Please note that security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[23]

[22] https://www.caara.org.au/wp-content/uploads/2020/07/Information-Management-Requirements-for-Software-as-a-Service-V1.0-May-2020.pdf

[23] See Section 12.1 for links.

7 Risk Management

Principle 7: **M365 must be regularly monitored for risk to records with areas of identified risk actively addressed**

REQUIREMENTS

24. Encryption of records by staff or external parties that is not authorised by the agency must be avoided where possible. This includes messages, email, and records with expiration dates or unauthorised password protection.

25. The agency must be able to demonstrate the integrity of records in the system (for example, using any checksum method that can demonstrate the record has not been altered, etc.)

26. Any virtualisation and multi-tenanted storage arrangements must be shown to be secure, and data must be segregated from other tenants appropriately. Agencies using a multi-tenanted service must be able to independently manage their tenancy.

27. Records identified by the agency as being vital must be provided with adequate protection from disasters. A disaster preparedness, management, and recovery programme for public records within agency-owned or -managed storage areas and facilities must be:

- developed
- implemented
- tested in accordance with programme requirements and timeframes
- updated based on the outcomes of the test.

28. Risks to records must be identified, managed, or mitigated as part of an executive endorsed agency-wide risk management program. Systems managing records flagged as having high risk and / or identified as having high value (whether to the agency, community, or other key stakeholders) must be protected by business continuity strategies and plans.

29. The agency must be able to regularly review the system to ensure it continues to meet their legislative and recordkeeping obligations. System audits must be able to test and validate management controls of systems, including information integrity, and corrective actions undertaken to address issues within required and appropriate timeframes

30. Services must be monitorable against contractual requirements and a suitable monitoring program put in place. Agencies must be able to demonstrate that records and information management is assessed in outsourced and service contracts, and that clauses in contracts or agreements are included where required. Timeframes must be appropriate, relevant, and related actions adequately tracked

31. Deviations from expected routine operations that affect information integrity, useability, or accessibility must be identified and tracked. The agency must be notified and provided with details of what occurred during the deviation. The interruption or issue must be resolved and documented.

7.2 General Implementation Advice

Risk to records may be prevented by regular monitoring and reviewing (both manually and through automated identification and alert processes). This includes regular monitoring and review of audit logs, access logs, security breaches, event logs, and the impact that changes Microsoft have made to M365 on the configuration, integration, and other design settings of an agency's specific business implementation. While some of these can be automated, others will need user intervention to make decisions and take responding actions.

Risks should be flagged, described, and mitigated in accordance with the agency's risk management frameworks and aligned with legislative, regulatory, business, and community requirements. Triggers for alert notifications, remediation actions, and other monitoring and reporting risk actions for once a risk has become an issue should be set in place.[24]

The Australian Cyber Security Centre provides resources to assist the assessment of cloud service providers[25]. Service providers are encouraged to participate in the Information Security Registered Assessors Program (IRAP)[26] to independently assess security compliance, suggest mitigations, and highlight residual risks regarding the cloud and other associated services they provide. Microsoft has participated in this program.[27]

7.1 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 7	**PROS 19/03 Strategic Management Standard** Principle 1 Valuing Records, Principle 6 Assessment and Measurement **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control	See **PROS 19/03 G Strategic Management Guideline** for information on assessment methods, and value / risk assessments. **PROS 19/04 G Operational Management Guideline** includes information about recordkeeping requirements and risk in relation to systems, processes, and contracts. The CAARA Paper on **Information Management Requirements for Software-as-a-Service**[28] includes risks related to software-as-a-service systems.
Requirement 24	**PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 20/02 Storage Standard** Principle 2 Protection and Security, and Principle 3 Survival as Readable Records	**PROS 19/04 G Operational Management Guideline** includes information about encryption in reference to access and security requirements. **PROS 19/05 S4 Constructing VEOs Specification** includes reference to encryption in relation to VERS Encapsulated Objects (VEOs), which are required for permanent digital records and recommended for long term temporary digital records. An understanding of Access Requirements (**PROS 19/06 Access Standard**), Storage Requirements (**PROS 20/02 Storage Standard**) and relevant jurisdictional Security Requirements are needed for this work

[24] The information management security manual may be of value when determining risk and appropriate actions and is available here: https://www.cyber.gov.au/acsc/view-all-content/ism

[25] https://www.cyber.gov.au/acsc/view-all-content/programs/irap/asd-certified-cloud-services accessed 29/08/2021

[26] https://www.cyber.gov.au/acsc/view-all-content/programs/irap accessed 17/08/2021

[27] https://docs.microsoft.com/en-us/compliance/regulatory/offering-irap-australia

[28] https://www.caara.org.au/wp-content/uploads/2020/07/Information-Management-Requirements-for-Software-as-a-Service-V1.0-May-2020.pdf

		Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[29]
Requirement 25	**PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 19/04 Operational Management Standard** Principle 1 System Planning and Procurement and Principle 2 System Maintenance	**PROS 19/04 G Operational Management Guideline** includes information about system requirements for preservation of the integrity of records. Information regarding what is needed for records to be full and accurate, as well as how long they should be kept for, will feed into this work.[30] Please note that VERS Encapsulated Objects[31] (see **PROS 19/05 S3 Long Term Sustainable Formats, PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification)** are designed to preserve the integrity of the records encapsulated.
Requirement 26	**PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 2 Protection and Security, and Principle 3 Survival as Readable Records	**PROS 19/04 G Operational Management Guideline** includes information about system requirements and contracting requirements, including sample clauses. The CAARA Paper on **Information Management Requirements for Software-as-a-Service**[32] includes questions to ask regarding services offered to multiple tenants regarding software-as-a-service systems.
Requirement 27	**PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 20/02 Storage Standard** Principle 2 Protection and Security, Principle 3 Survival as Readable Record, and Principle 4 Risk Managements	**PROS 19/04 G Operational Management Guideline** includes information about system requirements, including maintenance and transitioning between systems.[33] The CAARA Paper on **Information Management Requirements for Software-as-a-Service** includes disaster preparedness and business continuity for software-as-a-service systems.
Requirement 28	**PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 2 Protection and Security, and Principle 4 Risk Managements	An assessment against **PROS 19/03 Strategic Management Standard** will be needed to determine how the M365 implementation fits with the broader records management program, including aligned strategies, policies, and governance structures. Information on identifying value and risk in relation to records is in the **PROS 19/03 G Strategic Management Guideline**. Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[34]

[29] See Section 12.1 for links

[30] See the record disposal topic page for more information on record retention: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept

[31] See the VERS Topic Page for additional information: https://prov.vic.gov.au/recordkeeping-government/vers

[32] https://www.caara.org.au/wp-content/uploads/2020/07/Information-Management-Requirements-for-Software-as-a-Service-V1.0-May-2020.pdf

[33] Information on disaster management is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/disaster-management

[34] See Section 12.1 for links.

Requirement 29	**PROS 19/04 Operational Management Standard** Principle 1 System Planning and Procurement, especially Requirement 2 **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control, especially Requirement 2 **PROS 20/02 Storage Standard** Principle 3 Survival as Readable Record, and Principle 4 Risk Managements **PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation	An assessment against **PROS 19/03 Strategic Management Standard** will be needed to determine how the M365 implementation fits with assessment and measurement programs and aligned reporting programs. Please also see the **PROS 19/03 G Strategic Management Guideline** for information on setting record assessment and measurement programs. **PROS 19/04 G Operational Management Guideline** includes information about systems requirements to be monitored This may also link in with metadata[35] requirements located within **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification** An understanding of how long records need to be kept will feed into this work. Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.
Requirement 30	**PROS 19/04 Operational Management Standard** Principle 2 System Maintenance and Principle 5 Contracting **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 20/02 Storage Standard** Principle 3 Survival as Readable Record, Principle 4 Risk Managements and Principle 5 Use of External Storage Providers	**PROS 19/04 G Operational Management Guideline** includes information about contracts and agreements in relation to records management, including contract clauses for recordkeeping. Please see the **PROS 19/03 G Strategic Management Guideline** for information on setting record assessment and measurement programs The CAARA Paper on **Information Management Requirements for Software-as-a-Service** provides additional guidance regarding potential risks to records.
Requirement 31	**PROS 19/04 Operational Management Standard** Principle 1 System Planning and Procurement and Principle 2 System Maintenance **PROS 19/05 Create, Capture and Control Standard** Principle 3 Control **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 2 Protection and Security, Principle 3 Survival as Readable Records and Principle 4 Risk Management	**PROS 19/04 G Operational Management Guideline** includes information on system requirements and processes. An assessment against **PROS 19/03 Strategic Management Standard** may help with determining how deviations would be reported up and fit within assessment, reporting and other governance structures. Please also see the **PROS 19/03 G Strategic Management Guideline** for information on setting record assessment and measurement programs.

[35] Information on metadata is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/metadata

8 Disposal

Principle 8: **Disposal of records in M365 must be lawful**

REQUIREMENTS

32. Disposal of records in M365 systems must be authorised in accordance with the relevant recordkeeping authority requirements.

- Records must be sentenced according to current authorised retention and disposal authorities.
- All decisions to dispose of records must be formally endorsed by public sector employees with the appropriate authority and knowledge and documented. Disposal decisions must not be left to the end user or service provider.

33. The agency must account for the disposal of records or information created, captured, or managed in M365 systems in accordance with legal obligations and accountability requirements.

- Disposal of records must be documented in accordance with the requirements of the relevant recordkeeping authority.
- All disposal actions must retain a record of the event identifying the type of disposal and authorisation in accordance with the relevant recordkeeping authority requirements. For example, the system must retain a meaningful metadata 'stub', either in-place or in a register, when records leave the system or are destroyed. Records leaving the system must travel with contextual metadata.

34. The system must enable the identification of records and groups of records eligible for disposal and enable their disposal.

35. The agency must be able to reliably implement a freeze on disposal actions to ensure that records or groups of records required for legal actions are not disposed of until the legal action is concluded.

36. Where the system supports automated workflows for disposal, those disposal actions must not be executed without review by someone with the appropriate knowledge and authority within the agency to ensure that requirements have not changed.

37. Agencies must identify, address, and prevent any inappropriate ad hoc disposal mechanisms that the system implements (for example, storage quotas that enforce deletion or administrative functions that purge information at will). Note that enforced deletion may make the software unfit for purpose.

38. Policy, business rules, and procedures must identify how the destruction of records and information must be managed, including deletion of data.

- Methods used to destroy records must comply with relevant legislation, including privacy and confidentiality requirements.
- Methods used to destroy records must be irreversible and include destruction of all system copies of the record. An example would be media sanitisation where appropriate. The process chosen will depend on the risk and type of information.

8.1 General Implementation Advice

Records and information are kept for as long as they are needed for business, legal requirements (including in accordance with current authorised RDAs), accountability, and community expectations. Agencies are to maintain disposal documentation showing what records have been destroyed or otherwise disposed of, under what disposal instrument, who authorised the disposal, and when the disposal occurred.

Disposal decisions for records and information in M365 and associated systems and applications, including their destruction, should be managed in a lawful and timely manner by those with appropriate levels of authorisation and competency.

Metadata relevant to the record should travel with the record when they leave the system (for example, on transfer to the archival authority). Where records are destroyed through an authorised process, the metadata that remains in the system should note what the record was and what happened to it.

Where automation is in place to conduct disposal actions based on set triggers, there will need to be a step for someone with the relevant authority and knowledge to conduct a review of the disposal sentence prior to the initiation of the disposal. This is to ensure that the trigger is accurate and there has been no change (for example, because of a legal hold or disposal freeze, or due to the retention period changing).

8.1 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 8	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation	See PROV's general information on **record disposal**[36] **Retention and Disposal Authorities**[37] are required to ensure disposal is lawful.
Requirement 32	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation **PROS 19/04 Operational Management** Principle 3 Processes **PROS 20/02 Storage Standard** Principle 3 Survival as Readable Records	**PROS 19/03 Strategic Management Standard** feeds into this work. **PROS 19/03 G Strategic Management Guideline** provides guidance on recordkeeping governance and strategic planning (including documenting accountabilities and responsibilities). **PROS 19/04 G Operational Management Guideline** includes information on system functionality for disposal and setting processes.
Requirement 33	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation **PROS 19/04 Operational Management** Principle 3 Processes **PROS 20/02 Storage Standard** Principle 3 Survival as Readable Records	See PROV's general information on **record disposal** and **RDAs**. **PROS 19/03 Strategic Management Standard** feeds into this work. **PROS 19/03 G Strategic Management Guideline** provides guidance on recordkeeping governance and strategic planning (including documenting accountabilities and responsibilities). **PROS 19/04 G Operational Management Guideline** includes information on system functionality for disposal and setting processes.

[36] Information on record disposal is located here: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept

[37] Information on Retention and Disposal Authorities is located here: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas

Requirement 34	**PROS 22/04 Disposal Standard** Principle 2 Implementation **PROS 19/04 Operational Management** Principle 3 Processes **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 20/02 Storage Standard** Principle 3 Survival as Readable Records and Principle 4 Risk Management	**PROS 19/04 G Operational Management Guideline** includes information on system functionality for disposal See PROV's general information on **record disposal** and **RDAs**.
Requirement 35	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation **PROS 20/02 Storage Standard** Principle 3 Survival as Readable Records	**PROS 19/04 G Operational Management Guideline** includes information on system functionality for disposal See PROV's general information on **record disposal**
Requirement 36	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation **PROS 19/04 Operational Management** Principle 3 Processes	**PROS 19/03 Strategic Management Standard** feeds into this work. **PROS 19/03 G Strategic Management Guideline** provides guidance on recordkeeping governance and strategic planning (including documenting accountabilities and responsibilities). **PROS 19/04 G Operational Management Guideline** includes information on system functionality for disposal and setting processes. See PROV's general information on **record disposal** and **RDAs**.
Requirement 37	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation **PROS 19/04 Operational Management** Principle 3 Processes **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 3 Survival as Readable Records and Principle 4 Risk Management	**PROS 19/04 G Operational Management Guideline** includes information on system functionality for disposal See PROV's general information on **record disposal** and **RDAs**.
Requirement 38	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation **PROS 19/04 Operational Management** Principle 3 Processes	**PROS 19/04 G Operational Management Guideline** includes information on system functionality for disposal and setting processes. See PROV's general information on **record disposal** and **RDAs**. Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[38]

[38] See Section 12.1 for links

9 Migration

Principle 9:	**Records within M365 must be able to be migrated and exported to external systems as needed**

REQUIREMENTS	
39.	The system must provide effective export of selected records (including metadata) without loss of integrity.
40.	The ability to move information to other providers and products must be assessed in outsourced, cloud, or similar service arrangements.
41.	Migrated, converted, or reproduced information must be as authentic, reliable, and usable as the original source information from which it was created. This includes migration of event metadata and preservation of aggregations / relationships between records. The integrity of migrated records must be demonstrated. This requirement also applies to movement of records within the system, such as, from Teams to SharePoint.
42.	Once the records have been migrated, the system must be able to delete the records from the source location, retaining only a metadata stub, either in-place or in a register, to identify that the record had been in the system and what had happened to it.

9.1 General Implementation Advice

Records and information within M365 and associated systems and applications should be migrated to external systems as required in a manner that:

- retains their integrity as evidence of business
- retains their context
- ensures they remain accessible and useable
- follows relevant legislative and regulatory requirements

Records and information within M365 that are required for long-term use will need to be managed to ensure their long-term preservation. This includes the preservation of their integrity as evidence, as well as functionality that will enable the records and information to continue to be understood, accessed, and read.

9.1 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 9	**PROS 19/03 Strategic Management Standard** Principle 7 Transferring functions outside the Victorian Public Sector and Principle 8 Transferring functions between Victorian public offices **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve	**PROS 19/04 G Operational Management Guideline** includes information on system transition. See PROV's information on **migration**[39]
Requirement 39	**PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve, especially Requirement 3 **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 20/02 Storage Standard** Principle 3 Survival as Readable Record **PROS 22/04 Disposal Standard** Principle 2 Implementation	**PROS 19/04 G Operational Management Guideline** includes information on system transition, including functionality required to enable import and export. See PROV's information on **migration**
Requirement 40	**PROS 19/04 Operational Management Standard** Principle 1 System Planning and Procurement Principle 2 System Maintenance, especially Requirement 2, and Principle 5 Contracting **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 20/02 Storage Standard** Principle 1 Authorisation and Principle 4 Risk Management **PROS 22/04 Disposal Standard** Principle 2 Implementation	**PROS 19/04 G Operational Management Guideline** includes information on system transition, including functionality required to enable import and export, and on what to include in contracts and agreements, including sample contract clauses. See PROV's information on **migration**
Requirement 41	**PROS 19/04 Operational Management Standard** Principle 2 System Maintenance, especially Requirement 2 **PROS 19/05 Create, Capture and Control Standard** Principle 1 Create and Capture, and Principle 2	**PROS 19/04 G Operational Management Guideline** includes information on system transition, including functionality required to enable import and export This may also link in with metadata[40] requirements located within **PROS 19/05 S2 Minimum Metadata Requirements Specification; PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5**

[39] Information on migration is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/migration

[40] Information on metadata is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/metadata

	Preserve **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 20/02 Storage Standard** Principle 3 Survival as Readable Record **PROS 22/04 Disposal Standard** Principle 2 Implementation	**Adding Metadata Packages to VEOs Specification** See PROV's information on **migration** Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[41]
Requirement 42	**PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation	**PROS 19/04 G Operational Management Guideline** includes information on system transition, including functionality required to enable deletion. See PROV's information on **migration** An understanding of how long records need to be kept will feed into this work.[42]

[41] See Section 12.1 for links.

[42] See the record disposal topic page for more information on record retention: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept

10 Decommissioning

Principle 10:	Records must remain accessible and secure when decommissioning M365

REQUIREMENTS	
43.	Decommissioning of systems must consider retention and disposal requirements for records and information contained in the system.
44.	Decommissioning decisions must be formally documented and approved by a public sector employee with the appropriate authority and responsibility within the agency.
45.	Unmigrated records that are not authorised for disposal must be managed in a state that preserves their integrity, discoverability, and access for as long as they are required.

10.1 General Implementation Advice

When decommissioning M365 and / or associated systems and applications, the records and information should remain secure, accessible, and useable for as long as they are needed, in a manner that retains their integrity and contextual environment.

10.1 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 10	**PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve **PROS 19/06 Access Standard** Principle 3 Accessibility	**PROS 19/04 G Operational Management Guideline** includes information on system security functionality and access controls. See PROV's information on **decommissioning**[43] An understanding of how long records need to be kept will feed into this work.[44]
Requirement 43	**PROS 19/04 Operational Management Standard** Principle 2 System Maintenance **PROS 19/06 Access Standard** Principle 3 Accessibility	**PROS 19/05 S2 Long Term Sustainable Formats Specification** for formats required for permanent and recommended for long term temporary records. The retention period will need to be known to determine the best format to retain the record and preserve its integrity over time.[45]

[43] Information on decommissioning is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/decommissioning

[44] See the record disposal topic page for more information on record retention: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept

[45] Information on RDAs is located here: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas

	PROS 22/04 Disposal Standard Principle 1 Authorisation; Principle 2 Implementation	VERS Encapsulated Objects[46] (see **PROS 19/05 S3 Long Term Sustainable Formats, PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification)** are designed to preserve the integrity of the records encapsulated. See PROV's information on **decommissioning**
Requirement 44	**PROS 19/04 Operational Management Standard** Principle 2 System Maintenance **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 20/02 Storage Standard** Principle 1 Authorisation **PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation	**PROS 19/03 Strategic Management Standard** feeds into this work. **PROS 19/03 G Strategic Management Guideline** provides guidance on recordkeeping governance and strategic planning (including documenting accountabilities and responsibilities). **PROS 19/04 G Operational Management Guideline** includes information on system functionality required for authorisation. See PROV's information on **decommissioning**
Requirement 45	**PROS 19/04 Operational Management Standard** Principle 2 System Maintenance **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 20/02 Storage Standard** Principle 1 Authorisation, Principle 2 Protection and security, Principle 3 Survival as readable records and Principle 4 Risk Management **PROS 22/04 Disposal Standard** Principle 2 Implementation	**PROS 19/04 G Operational Management Guideline** includes information on system functionality required for disposal. The retention period will need to be known to determine the best format to retain the record and preserve its integrity over time. VERS Encapsulated Objects (see **PROS 19/05 S3 Long Term Sustainable Formats, PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification)** are designed to preserve the integrity of the records encapsulated. See PROV's information on **decommissioning** Security and privacy requirements specified by other Victorian bodies, such as Office of the Victorian Information Commissioner, will need to be applied.[47]

[46] See the VERS Topic Page for additional information: https://prov.vic.gov.au/recordkeeping-government/vers

[47] See Section 12.1 for links.

11 Transfer of Permanent Records

Principle 11:	Permanent records within M365 must be transferred to the relevant archival authority

REQUIREMENTS	
46.	Content of permanent records must be in an approved long-term and sustainable format (or can be easily, reliably, and cheaply converted to such a format that ensures it remains useable and authentic) and associated with sufficient metadata in accordance with the requirements of the relevant jurisdictional recordkeeping authority.
47.	The agency must be able to identify permanent value records and ensure they have the capability to extract and package them in accordance with archival authority specifications. The agency must be able to transfer them to the archival authority as legislation requires and within a time period that mutually agreeable between the agency and archival authority.

11.1 General Implementation Advice

Records required for preservation by relevant archival authorities are referred to as 'permanent value' records. They are identified through appraisal: the evaluation of government activities to specify what records should be made, determine how long records must be kept to meet the government's needs, support organisational accountability, and meet community expectations.

The agency must be able to comply with requirements for management of records defined as permanent value by the archival authority with jurisdiction over the records. Requirements usually include the timing and preparation of the records for transfer to the relevant archival authority.

11.1 Corresponding Requirements in PROV Standards

CAARA No.	PROV No.	Comments
Principle 11	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation; Principle 3 Transfer Obligations	Permanent records must be transferred to PROV in accordance with PROV requirements. See the **Transferring Records to PROV** topic page for more information.[48] Digital records must be transferred as VERS Encapsulated Objects[49] in line with **PROS 19/05 S3 Long Term Sustainable Formats, PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification**.

[48] Information on transferring records to PROV is located here: https://prov.vic.gov.au/recordkeeping-government/transferring-records

[49] See the VERS Topic Page for additional information: https://prov.vic.gov.au/recordkeeping-government/vers

Requirement 46	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation; Principle 3 Transfer Obligations **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve **PROS 19/04 Operational Management Standard** Principle 5 Contracting	The format that digital records must be transferred to PROV in is described in the following Specifications: **PROS 19/05 S3 Long Term Sustainable Formats, PROS 19/05 S4 Constructing VEOs Specification** and **PROS 19/05 S5 Adding Metadata Packages to VEOs Specification**. See PROV's general information on **metadata**[50] . See the **Transferring Records to PROV** topic page for more information
Requirement 47	**PROS 22/04 Disposal Standard** Principle 1 Authorisation; Principle 2 Implementation; Principle 3 Transfer Obligations **PROS 19/06 Access Standard** Principle 3 Accessibility **PROS 19/05 Create, Capture and Control Standard** Principle 2 Preserve **PROS 19/04 Operational Management Standard** Principle 5 Contracting	For information on how to appraise records to determine their value and therefore how long they need to be kept, see PROV's topic page on **Appraisal**.[51] Information on system requirements for disposal of permanent records is in **PROS 19/04 G Operational Management Guideline.** See the Transferring Records to PROV topic page for more information

[50] Information on metadata is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/metadata

[51] Information on appraisal is located here: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/appraisal

12 Useful Resources

12.1 Office of the Victorian Information Commissioner

Office of the Victorian Information Commissioner (OVIC) website home page (https://ovic.vic.gov.au)

OVIC have guidance on the **Information Privacy Principles** and how they are to be applied in public sector agencies.

They also have information on the **Victorian Protective Data Security Framework**, associated Standards, and guidance on how they are to be applied in the public sector, including reporting requirements.

OVIC have undertaken considerable research into the use of artificial intelligence, machine learning, deep learning and how they should be applied within the public sector.

12.2 Risk Management Framework

The framework is located on the Department of Treasury and Finance website (https://www.dtf.vic.gov.au/planning-budgeting-and-financial-reporting-frameworks/victorian-risk-management-framework-and-insurance-management-policy)

The Victorian Government Risk Management Framework applies to departments and public bodies covered by the *Financial Management Act 1994*.

The Framework describes the minimum risk management requirements agencies are required to meet to demonstrate that they are managing risk effectively, including inter�agency and state significant risk.

Detailed guidance, information and risk management support is available from the Victorian Managed Insurance Authority (https://www.vmia.vic.gov.au/tools-and-insights/risk-management-tools)

12.3 Information Management Framework

The framework and associated standards and policies are located on the Victorian Government website (https://www.vic.gov.au/information-management-whole-victorian-government).

The Information Management Framework (framework) provides a high-level view of government's information management landscape and a shared direction for government and agency information management practice.

12.4 Council of Australasian Archives and Records Authorities

Council of Australasian Archives and Records Authorities (CAARA) website (https://www.caara.org.au/)

Some products are located on the Australasian Digital Recordkeeping Initiative (ADRI) completed products page (https://www.caara.org.au/index.php/working-groups/adri/products/).

This includes *Information Management Requirements for Software-as-a-Service*. CAARA's *Information Management Requirements for Software-as-a-Service guidance* assists organisations in managing the risk of breaching legal and practical information management obligations, focusing on addressing this risk during the procurement of such systems.

13 Glossary of Terms

Term	Definition
Agency	An administrative unit which has or had responsibility for the provision of at least one aspect of government administration.
Appraisal	The process of evaluating business functions and activities to ascertain: • which records need to be created and captured • how long the records should be kept to meet business needs, organisational accountability, and community expectations
Authenticity	The record is what it claims to be, including who created or sent it and when.
Business classification scheme	A tool for linking records to the context of their creation.
Capture, of records	The processes involved in placing records into the appropriate systems, with the required metadata, so records can be managed properly and used over time as reliable evidence of actions and decisions.
Classification	Systematic identification and arrangement of business activities and / or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system.
Context	The information to sustain a record's meaning or evidential value. Context describes the who, what, where, and why of record creation and use.
Control, of records	The mechanisms imposed on records to ensure they are protected, provide reliable evidence of actions and decisions, are retained for the minimum required retention period, and can be accessed and used for authorised purposes. Control mechanisms include metadata, access restrictions, format requirements, system workflows, automated classification and sentencing, business rules, etc.
Destruction	Destruction renders records unreadable and irretrievable. Public records can only be destroyed or otherwise disposed of in accordance with standards issued by the relevant archival authority.
Disposal	The implementation of appraisal decisions authorised by retention and disposal authorities or other instruments. Disposal refers to the destruction or deletion of records from organisational systems; the migration of records between systems; and the transfer of records to the archival authority and / or to secondary storage.
Disposal authority	Disposal authorities are mandatory standards issued by the relevant archival authority and are a legal instrument authorising the disposal of public records. Disposal authorities ensure the disposal of public records is open, transparent, and accountable. They: • set the minimum retention time that different classes of records must be kept and how they are to be disposed • authorise the destruction of records which are no longer required (time-expired records) • identify records that are to be permanently retained as state archives.

Information Asset	A body of information and / or records that can be defined and managed as a single unit so it can be understood, shared, protected, and exploited effectively.[52]
Instrument	A formally issued document that governs and authorises records management or archival actions, such as a Disposal Authority.
Integrity	The record is complete and unaltered. Any authorised additions or annotations are explicitly indicated and traceable.
Long-term temporary record	A temporary public record which is required to be kept for a specific period of time that exceeds the life of the system managing it.
Metadata	Descriptive information about the content, context, structure, and management of records. It can be created, captured, and managed automatically by a piece of software or system, manually by a person, or by using a combined approach. Metadata about records may be held across a number of different systems within an agency, including recordkeeping and / or business systems.
Minimum Metadata	The minimum fields of metadata required by a jurisdictional authority to be associated with a record.
Permanent record	A public record which has been appraised by an archival authority as required to be kept as part of the jurisdiction's archives. Permanent records are specified in disposal authorities issued by the archival authority.
Persistent Metadata	Metadata that will remain attached to the record, for example, a machine-readable, long-lasting reference to a document, file, webpage, or other object
Record	A record is information in any format created, received, and maintained as evidence by an organisation or person, to fulfil legal obligations, or in the transaction of business.
Recordkeeping	Creating and maintaining complete, accurate, and reliable evidence of activities and decisions in the form of recorded information. Recordkeeping involves the design and management of processes and systems to capture full and accurate evidence of an organisation's activities.
Reliability	The contents of the record can be trusted as a full and accurate representation of the facts. The contents of the record can be depended upon by the agency, the government, and the community, and relied upon in legal proceedings.
Retention & Disposal Authorities (RDAs)	Standards issued by the archival authority that specify the records to be retained as permanent archives, and to authorise the disposal of records not required as archives once the defined minimum retention periods have been met. RDAs provide continuing authorisation without further approval from the archival authority. RDAs may apply to one or more agencies.
Sentenced	The process of identifying and classifying records according to the Retention & Disposal Authority and applying the specified disposal action.
Service Provider (Third-Party)	A third-party or outsourced supplier who provides a service to an agency or undertakes the implementation of a function or activity of government on behalf of an agency.

[52] GEA-NZ Information Asset Catalogue Guidelines v2.0 <https://archives.govt.nz/manage-information/how-to-manage-your-information/implementation/key-definitions>

Software as a Service (SAAS)	Any arrangement where a vendor uses their cloud infrastructure and cloud platforms to provide customers with software applications.
Temporary record	A public record which has been appraised by the archival authority as being required to be kept for a specific period of time for legislative or other requirements before it can be destroyed.
Useability	The record can be located, retrieved, and presented in a timely manner. It should be linked to any related records.

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 Standard