Functional Requirements for Managing Records in Microsoft 365

Version 1.0 October 2021

adri Australasian Digital Recordkeeping Initiative

CAARA
Council of Australasian Archives and Records Authorities
follow #caara

The Australasian Digital Recordkeeping Initiative (ADRI) is composed of representatives from all state and national archival authorities in Australia and New Zealand. ADRI is a Working Group of the Council of Australasian Archives and Records Authorities (CAARA).

Table of Contents

1 Introduction

This document sets out the functional requirements for managing records in Microsoft 365 and Office 365 based systems (hereafter referred to as M365). Records management and archival authorities are to reference the relevant disposal and other standards used in their jurisdiction when tailoring this document for their stakeholder needs.

1.1 Background

Public sector agencies are increasingly using M365 to create and manage their records.

While archival authorities and standard setting organisations have published requirements and guidance products for managing digital records, the scopes of these instruments have broadly targeted two types of systems: dedicated records systems or business systems.

- **Dedicated recordkeeping systems**, such as electronic document and records management systems (EDRMS) or enterprise content management systems (ECM), are designed to support metadata and mechanisms for secure, trustworthy, and accurate records. They are very controlled environments that function on a single point of truth. They often have hierarchical structures designed to enable controls to be placed onto records and to relate records to their functional context.
- **Business systems**, such as financial, human resources, or facilities management, are designed for a specific specialised purpose. They are designed to manage specific types of records with specialised metadata that will capture information related to that purpose and not necessarily capture all information needed for effective records management. For example, a finance system will be focused around effective management of financial data but may not capture information regarding retention periods for specific types of financial records.

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 and other organisations should be aware of the changes and actively monitor how changes may impact integration with other systems and business-specific configurations of M365.

1.2 Purpose of this document

This document provides high level principles and requirements for effective records management within M365. Please note that while many requirements relate to multiple principles, to minimise overlap requirements have been placed under the principle considered to be the area they are most needed.

Options for meeting the functional requirements include the following:

- native compliance – largely using functionality and configuration available within the M365 suite
- compliance through integration with a records management governance tool
- compliance through records (content and metadata) being pulled or pushed into a dedicated records management system (e.g. EDRMS or similar)
- some combination of the above options

These requirements may be met wholly or in part by the use of third-party products or organisational processes as long as the overall performance of the 'system' is compliant. The minimum requirements that an agency will need to meet will be dependent on their business needs, regulatory and legislative environment, and level of risk involved.

1.3 Audience

This document is 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.

It covers the following areas:

- For government and those working on behalf of government:
  - procurement
  - policy
  - information and communication technologies / information systems
  - information management / records management
  - cybersecurity / information security
  - audit, governance, compliance, risk management
- M365 and third-party product implementation and management.

1.4 Scope

This document 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.

M365 will be used throughout this document 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 the public records legislation of its jurisdiction.

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 document 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.

The requirements listed in section 2 of this document are highly recommended unless specified as being mandatory by the relevant records management authority. Where an agency opts not to implement a requirement, a risk assessment justifying their decision must be undertaken and fully documented.

1.5 Public records

Agencies must keep accurate and reliable information about their decisions, actions and agreements[1].

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. The relevant jurisdictional authority should be consulted for any exceptions.

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.

[1] The specific requirements vary depending on the jurisdiction.

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 data
- minutes from meetings (whether online or face-to-face)
- recordings of meetings
- posts on social media
- authorisations given via a system workflow
- information / data within a database.

A record comprises:

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

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.

1.6 Assumptions/prerequisites

This document assumes that the agency has an established records and / or information management framework in place based on recordkeeping best practice. 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)

This document also assumes that best practice recordkeeping (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).

Agencies must make and keep full and accurate records of business activity, appropriate to their business processes, regulatory environment, and risk and accountability requirements. 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.

Agencies must ensure information assets are linked to business functions and objectives (using metadata). Agencies 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.

The agency must ensure the systems they use meet their recordkeeping requirements and document the way in which they are addressed in each system. Such documentation may be subject to an audit of recordkeeping, and agencies may be required to provide this documentation to provide evidence that records are being managed appropriately.

Agencies should include records and information related risk in their risk management programs.

2 Functional Requirements

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

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

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.

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

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.

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

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.

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

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.

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

R21. 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.

R22. 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.

R23. 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.

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

R24. 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..

R25. 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.)

R26. 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.

R27. 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.

R28. 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.

R29. 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.

R30. 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.

R31. 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.

Principle 8: Disposal of records in M365 must be lawful

R32. 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.

R33. 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.

R34. The system must enable the identification of records and groups of records eligible for disposal and enable their disposal.

R35. 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.

R36. 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.

R37. 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.

R38. 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.

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

R39. The system must provide effective export of selected records (including metadata) without loss of integrity.

R40. The ability to move information to other providers and products must be assessed in outsourced, cloud, or similar service arrangements.

R41. 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.

R42. 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.

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

R43. Decommissioning of systems must consider retention and disposal requirements for records and information contained in the system.

R44. Decommissioning decisions must be formally documented and approved by a public sector employee with the appropriate authority and responsibility within the agency.

R45. 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.

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

R46. 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.

R47. 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.

3 Guidance

As components of evergreen systems, such as M365, will change over time, it is expected there will be an impact on how an agency meets the principles and requirements set out in this document. These requirements are therefore intended to be used throughout the life of the relevant systems and are not only for reference at the planning and implementation stages. They are criteria for a living 'as built' document that is maintained by the agency and updated to remain a verifiable model for the records management performance of the system.

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

When developing agency-specific measures that support the principles and requirements, care should be taken to ensure they are credible.

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

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 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.

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

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 or 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*[2] 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.

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

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.

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

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.

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

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 may need to be done manually.

---

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

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 ensures 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.

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

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.

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

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.[3]

[3] 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

Please note that the Australian Cyber Security Centre provides resources to assist the assessment of cloud service providers[4].. Service providers are encouraged to participate in the Information Security Registered Assessors Program (IRAP)[5] 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.[6]

Principle 8: Disposal of records in M365 must be lawful

Records and information are kept for as long as they are needed for business, legal requirements (including in accordance with current authorised records retention and disposal authorities), 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, as a result of a legal hold or disposal freeze, or due to the retention period changing).

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

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 in accordance with plans designed 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.

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

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.

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

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

[4] https://www.cyber.gov.au/acsc/view-all-content/programs/irap/asd-certified-cloud-services accessed 29/08/2021
[5] https://www.cyber.gov.au/acsc/view-all-content/programs/irap accessed 17/08/2021
[6] https://docs.microsoft.com/en-us/compliance/regulatory/offering-irap-australia

records should be made, determine how long records must to 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.

4 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 to 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.[7]
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.

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

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.
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.

5 Resources used

The primary resources used in the development of this document are the standards and specifications set by ADRI member archival authorities.

Those standards and specifications are informed by Australian and International Standards, in particular:

Creation, capture and management of records (e.g. ISO 15489)

Functional requirements for records in business systems (e.g. ISO 16175 pt.3 2010)

Functional requirements for digital records management systems (e.g. ISO 16175 pt.2 2011)

Additional SAAS-related requirements were drawn from the ADRI paper ‘Information Management Requirements for Software-as-a-Service’, v1.0 May 2020