GOVERNMENT OF WESTERN AUSTRALIA

Department of **Creative Industries, Tourism and Sport**
State Records Office of Western Australia

Records Management Advice

Record Keeping Governance for Microsoft 365

This document provides records managers and ICT managers with an overview of governance factors to consider with the configuration and use of Microsoft 365 (M365) in their organisations.

Introduction

Governance is a key element in the effective management of information and data (records) in M365. It comprises the policies, roles, responsibilities, and processes that guide how M365 is implemented and used in an organisation.

Information created or stored in M365 is considered a record under the *State Records Act 2000*, and organisations are responsible for managing these records regardless of whether M365 functions as a designated record keeping system.

What is M365?

M365 is a collection of subscription services and applications provided by Microsoft. Depending on the organisation's licencing plan with Microsoft, these include:

- Office applications for desktop, web and mobile productivity
- email and calendaring services in Exchange
- collaboration tools including Teams, SharePoint and Yammer
- file hosting and sharing services, such as OneDrive and SharePoint
- productivity tools such as OneNote and Planner
- security and compliance tools, including Purview
- business analytics tools.

1. Information Governance Framework for M365

Organisations should establish a clear governance framework to guide the use, architecture and configuration of the Microsoft 365 tenant as it relates to information management. This framework should include:

- Defined roles, responsibilities and decision-making processes for oversight of information stored in M365. Stakeholders in decision-making should include records, ICT, governance and user representatives.
- Ongoing monitoring of the M365 environment to ensure configurations remain current, effective and aligned with business and compliance requirements, noting that M365 is a rapidly evolving platform (“evergreen”).
- Organisational policies identifying which M365 services or applications are used to create and capture records, and how the records are managed. These should then be listed in the organisation record keeping plan (RKP) required under SRC Standard 2: Record Keeping Plans.
- Organisational policies and procedures describing how information stored in applications not considered as record keeping systems (RKS) e.g. individual and shared accounts for OneDrive, OneNote, Outlook, Forms and PowerBI is captured into the organisational RKS.
- Organisational policies and procedures that define roles and responsibilities for searching and retrieving content in M365 to comply with information access requests via Freedom of Information (FOI) and legal discovery.
- Processes that address the full lifecycle of information from creation to disposal, including the management of content associated with individual user accounts when employees leave the organisation e.g. Outlook, OneDrive, OneNote, Forms.

2. Provisioning of M365

Key considerations when configuring and preparing the M365 environment include:

- Licensing tiers and how they affect compliance functionality, noting that some roles – such as Records Management – may require advanced licence types e.g. E5 to manage classification, retention, review and disposition if M365 is an RKS.
- Default settings for services such as SharePoint, Teams, OneDrive and Exchange, particularly those affecting retention and storage e.g. default automatic recording of meetings in Teams creates records which will have to be managed in accordance with the General Retention and Disposal Authorities (GRDA).
- Controlled creation of SharePoint sites and Teams to support consistent configuration, ownership, naming conventions, and to reduce information sprawl.
- Retention settings aligned with the requirements outlined in retention and disposal authorities. For example, applying “retain forever” policies results in unnecessary long-term storage and costs, as well as the continued retention of documents that should have been disposed of which exposes organisations to additional FOI or litigation risks. Large volumes of unmanaged data will also create future disposal challenges.

- Classifications and sensitivity labels that align with the Western Australian Information Classification Policy.
- Metadata requirements and permission structures for SharePoint and Teams sites if used as an RKS. See Records Management Advice – Metadata for more information.

3. Security and Access Management

A structured permissions model should define who can access information, to what level and under what circumstances. These include:

- Establishing rules for external sharing, which may involve disabling external access by default and approving exceptions.
- Regular review of user permissions to ensure access remains appropriate, including the removal of access for users who change roles or leave the organisation.

4. Retention and Disposal

The disposition of content stored in M365 involves the deletion of temporary State records or the permanent retention of State archives.

Active records management should address records created or stored in:

- Outlook: personal and shared / group mailboxes
- SharePoint: standalone sites or sites associated with a Teams
- OneDrive
- OneNote: personal and shared / group
- Teams channel posts and 1:1 chats
- Forms: personal and shared / group

These must be managed in accordance with SRC Standard 8 Managing Digital Information and the relevant retention and disposal authorities. See Retention and Disposal of State Records for further information.

Organisations should be mindful of M365 retention policies and how they differ, interact or must be managed to meet the requirements outlined in retention and disposal authorities.

5. Change Management and Training

Organisations should provide training that supports employees in understanding policies, procedures and responsibilities relating to the management of records in M365.

The training should include advice on appropriate use of personal repositories of information such as Outlook, OneDrive, OneNote, Forms etc to ensure appropriate capture into an RKS.

Organisations may refer to the Information Governance Maturity Model for M365 to self-assess and identify areas for improvement. https://irms.org.uk/supporting-our-profession/resources/information-governance-maturity-model-for-m365/

For more information on managing records in M365, refer to

- Managing Records in Microsoft 365: A guide for Victorian public offices. https://prov.vic.gov.au/recordkeeping-government/document-library/guideline-managing-records-microsoft-365
- Microsoft 365 and recordkeeping https://www.nsw.gov.au/nsw-government/recordkeeping/secure-and-store/microsoft/m365-specifications