Microsoft 365 Guide

June 2020

Te Rua Mahara o te Kāwanatanga
ARCHIVES
NEW ZEALAND
Part of the Department of Internal Affairs
New Zealand Government

Document details

Document Identifier: 20/G18

Version	Date	Description	Revision due
1.0	June 2020	Final publication version	June 2022
1.1	Aug 2020	Minor edit to section 1.2	June 2022
1.2	Nov 2020	Reformatted. Privacy Act annotation.	June 2022

Contact for enquiries

Government Recordkeeping Directorate
Archives New Zealand
Phone: +64 4 499 5595
Email: rkadvice@dia.govt.nz

Acknowledgement

This document is based on the work undertaken and advice provided by the Public Records Office of Victoria (PROV), Australia.

Licence

Microsoft 365 Guide

1.1 Introduction

This guide is designed to assist public offices and local authorities adopting Microsoft 365 services. Microsoft 365, previously known as Office 365, is a suite of online products that includes SharePoint Online and is provided as a set of cloud-based subscription services. The subscription includes automatic software updates, which means that subscribers always have access to the latest version.

Software services commonly part of Microsoft 365 suite include:

- email services (e.g. Outlook Mail, Outlook Calendar, Outlook People, Outlook Tasks and Clutter)
- hosted services (e.g. Exchange, Skype for Business, SharePoint Online, and the browser-based Office Web Apps suite)
- Office applications (i.e. access to the current versions of the Office desktop applications)
- collaboration tools (e.g. OneDrive for Business, SharePoint Online, Microsoft Teams, Stream, Yammer, Skype for Business, Outlook Online and Delve boards).

1.2 Compliance

As with many software implementations, in its vanilla roll-out form Microsoft 365 is **not** compliant with the *Information and records management standard (16/S1)* (the *Standard)* or the *Public Records Act 2005* (the *PRA*). The implications of Microsoft 365 for information and records management in your organisation will depend on how the software is configured, the type of license held and whether or not Microsoft 365 is integrated into an electronic document and records management system (EDRMS) or enterprise content management system (ECMS).

To move towards compliance requires:

- developing a knowledge of the administrative applications and tools used to manage information and records in Microsoft 365
- understanding where and how things are stored across the Microsoft 365 suite; this includes not just how different applications behave, but whether or not off-shore storage is appropriate for your business
- a close working partnership between information and records management staff and the organisation's IT services
- identifying the appropriate level of governance licencing for your organisation
- closing gaps in capability by using 3rd party add-ons for information and records management (ECMS or EDRMS) functionality
- awareness of Microsoft 365 information and records management functionality and how it can be used to manage disposal of information and records
- in conjunction with your IT support, planning to monitor and aggressively manage your instance of Microsoft 365 over time as Microsoft's delivery method of updates and enhancements may impact on the operability of the compliance measures you may have implemented
- planning for and, where appropriate, implementing the opportunities Microsoft 365 provides to automate many information and records management processes.

The *Standard* sets clear expectations on the public sector for managing information and records. The Minimum Compliance Requirements contained in the *Standard* (supported by the *Implementation guide 16/G8)*) apply to the Microsoft 365 environment as they do with any system that creates and manages public or local authority records. The table at the end of this document highlights Minimum Compliance Requirements relating to an implementation of Microsoft 365.

1.3 How controls can be applied

Ideally, information and records management controls should be included during the planning and configuration stage. If this does not happen then various controls can be introduced post-implementation, but it is preferable to design these in at that start rather than retrofit. Key controls are listed below:

- labels and labelling policies can be used to manage retention of information and records and security regimes, including sensitivity classifications (note that content can have one retention and one sensitivity label applied at the same time)
- automated labelling can be applied, but currently only comes with the Enterprise E5 licence (as of Q3 2020)
- electronic approval processes can be set up using the Power Automate service (previously known as Flow), where agencies have established that electronic approval will meet their needs and obligations
- access permissions can be applied through SharePoint Permissions to sites, libraries and to groups, or through an Azure Information Protection label assigning usage rights protection to specific documents (if they need to remain secure regardless of where they are stored)
- unique IDs for documents can be set up within SharePoint Online using the automatic SharePoint Document ID functionality, but this is not the default and the functionality must be activated by a site administrator
- alerts can be set up or customised to advise of unauthorised deletions, changes, and amendments
- standardised metadata can be applied through site scripts and site designs for common sites, such as Team sites, Project sites
- eDiscovery tools that search all content, including email, can be set up through the Security and Compliance Centre (note that for some eDiscovery functionality a Microsoft 365 E5 license is currently required).

1.4 Disposal

If the Microsoft 365 service is integrated with an EDRMS or ECM system, then disposal controls can continue to be applied in that system through traditional methods (such as assigning retention periods through the business classification scheme and folder structure).

If there is no integration, disposal will need to be managed within Microsoft 365 and SharePoint Online, which uses a slightly different approach.

Disposal in Microsoft 365 environments can be **managed through setting retention policies in the Security and Compliance Centre**. These may be set up and applied through either of the following:

- classification through use of labels and labelling policies
- Data Governance-Retention via a retention policy.

Classification using labels and labelling policy can be automated with an E5 license. Otherwise the labels must be manually applied, which requires the user to select an appropriate label to apply where multiple labels exist. To do this the user must be aware of the agency's retention policy in order to select the appropriate label for their data.

Using the Data Governance application may be a better approach as it enables retention to be applied "behind the scenes" without user action. When applying retention policies, **consider the most appropriate level to apply the policy to**. For example:

- if applying at a high group level it may be useful to flatten retention periods to a few big buckets that round retention up to the relevant disposal class with the longest minimum required retention period, aligning with the settings in most disposal authorities issued under the *PRA*
- if everything except a couple of records is subject to one retention period, a separate retention for those records may be applied at the document level; however, this can be very onerous and document level retention is not usually advised.

1.5 Risks

1.5.1 ...to meeting legislative requirements

challenge

Information and records remain subject to privacy, security, official information (OIA and LGOIMA) and public records requirements while they are held externally in Microsoft 365 and SharePoint Online systems.

mitigation

Either integrate Microsoft 365 with a compliant system or configure Microsoft 365 in line with information and records management requirements to identify high risk areas and their appropriate mitigation.
For example, information and records above a specific security classification may need to be only created or stored on systems that are under direct agency control.
While a protected cloud environment may be an option for some information and records, others may not be permitted to be stored within an encrypted environment.

1.5.2 ...to evidential integrity of information and records, unauthorised access and unlawful deletion

challenge

The collaborative design of Microsoft 365 places the user in a position of decision maker regarding management of information and records when most users lack the skills and knowledge to manage them appropriately.

mitigation

Have information and records management controls (automated where possible) in place to ensure the evidential integrity of information and records, that they remain accessible, and that they are not subject to unauthorised access or unlawful disposal.
For example, use sensitivity labels, an associated and relevant Label Policy and audit log alerts to notify the appropriate person if unauthorised access occurs.

1.5.3 …to full and accurate records of government

challenge
It may be unclear who owns or holds what rights over the information and records in Microsoft 365 environments, including rights over information and records contained in laws from the jurisdiction where they are being held.

mitigation
Clarify ownership and rights over agency information and records and, where there is lack of clarity, ensure that they are held within agency owned and controlled systems. This clarification should also take into account the rights and interests that third parties might have in the information or records, for example iwi groups or others with intellectual property rights over public or local authority records.
For example, clearly express information and records ownership and rights in contracts and agreements.

1.5.4 …of losing information and records

challenge
Content may be lost due to Microsoft service changes, as part of normal service operations that include automated deletion, or upon removal of the service by Microsoft.

mitigation
Review and remain up to date with service changes including release notices to ensure that risk to information and records is known.
For example, if a Microsoft notice flags that a service will be disabled, review and either move or convert information and records from that service to one that is being actively managed.

1.6 Other considerations

Microsoft 365 is a cloud service that uses web-based applications (including forms of social media). As such, information and records management advice for cloud computing, management of websites, social media, mobile technologies and decommissioning systems also apply.

Information and Records Management Standard (16/S1)

The *Standard* provides Minimum Compliance Requirements. Listed below are those sections which are particularly relevant to the management of Microsoft 365.

Minimum Compliance Requirement from the Standard	Explanation from the *Implementation Guide*	Allows the organisation to…
Principle 1: Organisations are responsible for managing information and records		
1.5 Business owners and business units must be responsible for ensuring that information and records management is integrated into business processes, systems and services.	An organisation must identify business owners and system owners who are responsible for ensuring information and records management is included in all systems and processes used. Those owners must be aware that information and records management requirements are needed when they move to a new service environment, develop new business processes, systems or services, or improve on existing business processes, systems or services. Responsibilities for business owners must be identified and assigned in policies and within performance plans. Business owners must demonstrate that they have considered information and records management requirements and assessed risks as part of the development process. This requirement places responsibilities more broadly within an organisation. It reflects a business manager's detailed understanding of the information and records produced by and necessary to perform their work, and their responsibility for ensuring its management. Cascading responsibility to different business areas of the organisation lets business unit staff and information and records staff work together to ensure that information and records management is integrated into business processes, systems and services.	Associate information objects and/or record aggregations to their business context and support ongoing links to business context through business changes over time.
1.7 Information and records management responsibilities must be identified and addressed in all outsourced and	An organisation must ensure that information and records management is addressed in all service contracts, instruments and arrangements.	Ensure ownership of any records and information created under a contractual agreement is identified and conforms to jurisdictional, disposal, privacy and other legislative requirements.

Minimum Compliance Requirement from the *Standard*		Explanation from the *Implementation Guide*	Allows the organisation to…
	service contracts, instruments and arrangements.	An organisation's strategy and policy must include responsibilities to ensure that information and records requirements are identified and addressed. An organisation must undertake risk assessments and address information and records management risks in contracts, instruments and arrangements that it agrees to. Service contracts, instruments and arrangements include: • functions, activities or services of the organisation being outsourced to an external provider • functions, activities or services being moved to cloud services or other service providers (internal or external to the New Zealand public sector). An organisation must ensure that the portability of information and records and associated metadata is assessed and appropriately addressed in outsourced and service contracts, instruments and arrangements.	
1.8	Information and records management must be monitored and reviewed to ensure that it is accurately performed and meets business needs.	An organisation must regularly monitor information and records management activities, systems and processes to ensure they are meeting the needs of the organisation and conforming to requirements. Any issues identified though a monitoring process must be addressed in a corrective action plan. An organisation must monitor activities such as process and system audits of systems that are high-risk, high-value, or both. Any system of assurance for information and records management should be integrated into the wider organisational assurance processes. The Executive Sponsor has responsibility for overseeing this monitoring.	Produce reports that can be used to monitor destruction, storage and use for management and audit purposes. (Can be used to support organisational leadership to demonstrate effective and legally compliant information management).
Principle 2: Information and records management supports business			
2.1	Information and records required to support and meet business needs must be identified.	This requirement provides the foundation for managing information and records in all environments.	Document and maintain systems design and configuration within the system. This could include setup and changes to digital decision-making tools like algorithms, artificial

Minimum Compliance Requirement from the *Standard*	Explanation from the *Implementation Guide*	Allows the organisation to…
	By appraising its functions and activities, an organisation can identify what information and records it needs to support business. It can also identify other requirements, including Treaty of Waitangi / Te Tiriti o Waitangi obligations, and government and community expectations. This work provides the foundation for understanding what information and records to keep. It identifies what systems and business processes are high-risk, high-value, or both for the organisation, and the information and records required to support these. An organisation must incorporate this work into comprehensive and authorised disposal authorities for its information and records An organisation must document in its business rules, policies and procedures decisions about what information and records are required. The decisions must also be reflected in specifications for systems and metadata schema.	intelligence and integrated databases, including those built into analytics, workflow and search.
2.2 High risk/high value areas of business, and the information and records needed to support them, must be identified and regularly reviewed.	An organisation must identify the areas of high risk, high value, or both of its business. An organisation can better prioritise how it manages, treats and protects these critical systems and the information and records they contain. An organisation must identify the likely or potential risks to information and records management and manage or mitigate them. This includes protecting the systems that manage information and records that are high-risk, high-value, or both, from loss and damage. An organisation should set up appropriate security measures and business continuity strategies and plans. By identifying high-value information and records at creation, an organisation can better manage and use this core asset.	Migrate or export information or aggregations without losing context (metadata). Required when systems are implemented or decommissioned, or agencies merge. Test that the integrity of the records and key metadata is not degraded during migration and export. For example, content must be able to be exported/migrated more than once.
2.3 Information and records management must be design components of all	In complex business and systems environments, it is important to design information and records management at the start. This is particularly	Capture core metadata. At a minimum, the metadata specified in the *Standard.*

Minimum Compliance Requirement from the *Standard*	Explanation from the *Implementation Guide*	Allows the organisation to…
systems and service environments where high risk/high value business is undertaken.	important where the business involved is high-risk, high-value, or both. Include information and records management when you specify systems and service environments which manage high-risk and/or high-value information and records. You will be better able to manage and use the information and records. An organisation must consider at the start how to make system maintenance, migrations and decommissioning easier. In taking this “by design approach”, an organisation must ensure: • systems specifications for information and records that are high-risk, high-value, or both, include requirements for managing them • systems specifications include requirements for minimum metadata needed to support information and records identification, usability, accessibility and context • it keeps documents about systems design, configuration and any changes made over time. Migrating and decommissioning systems can be expensive and time-consuming. An organisation may hold insufficient documentation about: • the information and records held in the system • the configuration of the system • the disposal requirements for information and records held in the system.	Capture and maintain core process metadata to record the use of information or record aggregation. Assign and persistently link unique identifiers to each information object and record aggregation. This requirement must not undermine the restrictions on assigning unique identifiers to individuals under the Privacy Act 1993[1]. Document and maintain systems design and configuration within the system. This could include setup and changes to digital decision-making tools like algorithms, artificial intelligence and integrated databases, including those built into analytics, workflow and search.
2.5 Information and records management must be designed to safeguard information and records with long-term value.	This requirement ensures that an organisation identifies which systems and service environments hold information and records with identified long-term value. This requirement builds on *Minimum Compliance Requirements 2.1 and 2.2.* Once the organisation knows what information and records are needed long-term and where they are kept, it can safeguard and manage them.	Associate information objects and/or record aggregations to their business context and support ongoing links to business context through business changes over time. Identify information or record aggregations of information of long-term value (i.e. the information needs to remain accessible for more than 10 years). This is to ensure that

[1] Note: There is a new Privacy Act, this guide to be updated.

Minimum Compliance Requirement from the *Standard*	Explanation from the *Implementation Guide*	Allows the organisation to…
	Information and records required for the long term will outlive both the systems in which they are managed and any outsourcing arrangements and contracts with service providers. An organisation must ensure it plans and manages the protection of long-term information and records during transitions of systems and changes to service arrangements. Two such transitions are system migrations and decommissioning systems processes. Two such changes to service arrangements are termination of services and new outsourcing arrangements. An organisation must protect its long-term information and records during changes in administration and through changes in the machinery of government. This includes where information and records must be transferred between organisations. To help with identifying long-term information and records, an organisation can refer to their authorised disposal authorities.	organisations are able to maintain access via migration or format change. We suggest long term value equates to retention for more than 10 years for digital information.
2.6 Information and records must be maintained through systems and service transitions by strategies and processes specifically designed to support business continuity and accountability.	This requirement ensures that information and records are managed appropriately through system migrations and service transitions. Two examples are upgrades of systems and services offered in cloud environments. An organisation must have documented migration strategies, and appropriate planning and testing processes. These must ensure that information and records are not “left behind” or disposed of unlawfully. An organisation must use a managed process to migrate information and records and associated metadata from one system to another. The process must be managed to deliver records that are accessible, reliable and trustworthy. Maintaining appropriate system documentation will help to make migration strategies successful. An organisation must use migration and decommissioning processes that ensure that	Associate information objects and/or record aggregations to their business context and support ongoing links to business context through business changes over time. Identify information or record aggregations of information of long-term value (i.e. the information needs to remain accessible for more than 10 years). This is to ensure that organisations are able to maintain access via migration or format change. We suggest long term value equates to retention for more than 10 years for digital information. Migrate or export information or aggregations without losing context (metadata). Required when systems

Minimum Compliance Requirement from the *Standard*	Explanation from the *Implementation Guide*	Allows the organisation to…
	information and records are kept for as long as needed for business, legal requirements (including in line with authorised disposal authorities), and government, and community expectations. This requirement builds on *Minimum Compliance Requirement* 2.2 and *Minimum Compliance Requirement* 2.5. They require that information and records that are high-risk, high-value, or both, are supported and migrated appropriately. The portability of information and records and associated metadata must be assessed in outsourced or service arrangements. Information and records must not be "left behind" in outsourced arrangements. Such arrangements must include provisions for transferring the information and records back to the organisation.	are implemented or decommissioned, or agencies merge. Test that the integrity of the records and key metadata is not degraded during migration and export. For example, content must be able to be exported/migrated more than once. Document and maintain systems design and configuration within the system. This could include setup and changes to digital decision-making tools like algorithms, artificial intelligence and integrated databases, including those built into analytics, workflow and search.
Principle 3: Information and records are well managed		
3.2 Information and records must be reliable and trustworthy.	An organisation's information and records must have enough metadata to ensure they are reliable and trustworthy. Information and records must be accurate, authentic, and reliable as evidence of transactions, decisions and actions. This requirement ensures that information and records have appropriate minimum metadata to provide meaning and context (including te reo Māori), and that this metadata remains associated or linked. Do regular assessments or audits to demonstrate that management controls of business rules, procedures and systems are operating correctly. This provides assurance of the integrity of the information and records stored in the system. This requirement builds on the earlier principles in the *Standard*.	Capture core metadata. At a minimum, the metadata specified in the *Standard*. Capture and maintain core process metadata to record the use of information or record aggregation. Migrate or export information or aggregations without losing context (metadata). Required when systems are implemented or decommissioned, or agencies merge. Test that the integrity of the records and key metadata is not degraded during migration and export. For example, content must be able to be exported/migrated more than once.
3.3 Information and records must be identifiable, retrievable, accessible and	Information and records must be identifiable, retrievable from storage (physical or digital), and	Capture core metadata. At a minimum, the metadata specified in the *Standard*.

Minimum Compliance Requirement from the *Standard*	Explanation from the *Implementation Guide*	Allows the organisation to...
usable for as long as they are required.	accessible, usable and reusable for as long as required. To maintain the accessibility and usability of physical information and records, an organisation must store them in appropriate storage areas and conditions. To maintain the accessibility and usability of digital information and records, an organisation must ensure it regularly migrates or moves them from one system or platform to another. An organisation must associate or link appropriate minimum metadata (including te reo Māori terms) to information or records to ensure the information and records can be identified, retrieved and shared. An organisation must regularly test systems and perform assessments or audits to demonstrate that the systems can locate and produce information and records that people can read and understand. This requirement builds on the earlier principles in the *Standard*.	Capture and maintain core process metadata to record the use of information or record aggregation. Assign and persistently link unique identifiers to each information object and record aggregation. This requirement must not undermine the restrictions on assigning unique identifiers to individuals under the Privacy Act 1993[2]. Identify information or record aggregations of information of long-term value (i.e. the information needs to remain accessible for more than 10 years). This is to ensure that organisations are able to maintain access via migration or format change. We suggest long term value equates to retention for more than 10 years for digital information. Ensure a digital preservation plan can be applied to this information and record aggregation of long-term value without degradation and while maintaining relationships between exported components and their associated metadata. This is likely to entail format migration or export/migration of content, maybe more than once. Migrate or export information or aggregations without losing context (metadata). Required when systems are implemented or decommissioned, or agencies merge.

[2] Note: There is a new Privacy Act, this guide to be updated.

Minimum Compliance Requirement from the *Standard*	Explanation from the *Implementation Guide*	Allows the organisation to...
		Test that the integrity of the records and key metadata is not degraded during migration and export. For example, content must be able to be exported/migrated more than once. Ensure that information is securely stored and remains accessible over the time required to meet minimum retention periods. Enable content search in order to make information accessible and usable. This would typically include a variety of search and retrieval methods, including simple and advanced search, etc.
3.4 Information and records must be protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction.	An organisation must protect information and records. An organisation must implement an information security policy and appropriate security mechanisms. The policy must cover information and records held physically or digitally, or both. Security measures must include: • access and use permissions in systems • processes to protect information and records no matter where they are located, including in transit and outside the workplace • secure physical storage facilities. Undertaking regular assessments or audits will help an organisation verify that access controls have been implemented appropriately and are working.	Capture and maintain core process metadata to record the use of information or record aggregation. Fix and protect content and metadata from unauthorised alteration and deletion. Produce reports that can be used to monitor destruction, storage and use for management and audit purposes. (Can be used to support organisational leadership to demonstrate effective and legally compliant information management). Apply security and access permissions ensuring that only authorised users can access information appropriate to their access rights. Assign and actively manage government security classifications (NZISM).
3.5 Access to, use of and sharing of information and records must be managed	This requirement builds on the requirements in Part 3 of the Public Records Act 2005.	Apply security and access permissions ensuring that only authorised users can

Minimum Compliance Requirement from the *Standard*	Explanation from the *Implementation Guide*	Allows the organisation to…
appropriately in line with legal and business requirements.	An organisation must ensure that access to, use and sharing of information and records are in line with legal requirements including: • the *Official Information Act 1982* • the *Local Government Official Information and Meetings Act 1987* • the *Privacy Act 2020* • the *Health Information Privacy Code 1994* • organisational policies, business rules and procedures. Undertaking regular assessment s or audits of systems will help an organisation verify that access to, use and sharing of information and records is managed in line with business requirements, legal obligations and the Government ICT Strategy or Action Plan (where appropriate).	access information appropriate to their access rights Assign and actively manage government security classifications (NZISM)
3.6 Information and records must be kept for as long as needed for business, legal and accountability requirements.	An organisation must implement policies, business rules and procedures to ensure that information and records are kept for as long as required, and to identify how their disposal is managed. The policies, business rules and procedures must be in line with the requirements of the *Public Records Act 2005* and authorised disposal authorities. Information and records must be sentenced and disposed of in line with the practices of authorised disposal authorities. This includes information and records located in business systems, in outsourced or service arrangements, or in physical storage. Disposing of digital information and records may be part of a planned migration process or the decommissioning of systems. Information and records of permanent value that are identified as public or local authority archives must be transferred to Archives New Zealand, an approved repository or a local authority archive, when authorised and no longer needed for business purposes.	Ensure a digital preservation plan can be applied to this information and record aggregation of long-term value without degradation and while maintaining relationships between exported components and their associated metadata. This is likely to entail format migration or export/migration of content, maybe more than once. Schedule information and record aggregation for deletion (by an authorised person). Must allow for complete obliteration of content and all components of the information object such that it cannot be restored. Maintain an auditable record of disposal actions (including key metadata documenting disposal action). Ensure that information is securely stored and remains accessible over the time required to meet minimum retention periods.

Minimum Compliance Requirement from the *Standard*	Explanation from the *Implementation Guide*	Allows the organisation to…
3.7 Information and records must be systematically disposed of when authorised and legally appropriate to do so.	An organisation must implement policies, business rules and procedures that identify how the disposal of information and records is managed. This includes: • assigning responsibility for sentencing and disposal of information and records (sentencing is using a disposal authority to decide whether to keep, destroy or transfer a record) • using disposal authorisation processes • implementing disposal actions • deleting metadata • decommissioning systems • documenting the disposal of information and records. An organisation must be able to account for their disposal of information and records in business systems, outsourced arrangements, and physical storage. This includes providing evidence that the disposal of information and records is permitted and authorised under disposal authorities' and legal obligations, including the *Public Records Act 2005*.	Capture and maintain core process metadata to record the use of information or record aggregation. Schedule information and record aggregation for deletion (by an authorised person). Must allow for complete obliteration of content and all components of the information object such that it cannot be restored. Schedule information and record aggregations for transfer to an approved archive (including key metadata documenting transfer action). Maintain an auditable record of disposal actions (including key metadata documenting disposal action). Be able to stop the disposal process (sometimes referred to as a "legal hold" process"). Ensure that information is securely stored and remains accessible over the time required to meet minimum retention periods.