Microsoft

Meeting compliance requirements with Microsoft 365

Guidance for Western Australian Government agencies.

For more information on any of these capabilities please contact your Microsoft Account Team:

Glenn Winton
Account Executive
glennwi@microsoft.com

Mark Randell
Account Technology Strategist
mark.randell@microsoft.com

Antoinette Jago
Modern Work & Security Specialist
ajago@microsoft.com

Michael Gadsden
Account Executive
mgadsden@microsoft.com

Charles Poulsen
Account Technology Strategist
charles.poulsen@microsoft.com

Beau Faull
Security and Compliance Specialist
beau.faull@microsoft.com

Michael Richards
Security and Compliance Specialist
michael.richards@microsoft.com

The management of data security, classification, retention, disposal, searching, and regulatory requirements is a key topic of discussion amongst WA Government agencies. The increased digitisation of records and use of collaboration tools along with WA Government initiatives such as the Data Classification policy[1] and the State Records Office work on EDRMS in Office 365[2] are some items driving these discussions.

This document is part of a series of whitepapers intended as a guide for WA Government Agencies to clearly outline functionality that can be obtained from the broader Microsoft products and services.

Document Title	Version and Date
Essential Eight on a Page http://aka.ms/ausec/e8wagov	1.0, November 2021
Meeting Essential Eight requirements with Microsoft Security http://aka.ms/ausec/e8wpwagov	1.0, November 2021
Microsoft 365 Compliance on a Page http://aka.ms/ausec/compwagov	1.0, November 2021
Meeting compliance requirements with Microsoft 365 http://aka.ms/ausec/compwpwagov	1.1, November 2021
Microsoft 365 Security on a Page http://aka.ms/ausec/secwagov	1.0, November 2021
Meeting security requirements with Microsoft 365 http://aka.ms/ausec/secwpwagov	1.0, November 2021

Microsoft 365 compliance solutions provide integrated, intelligent tools to reduce risks without compromising worker productivity. These tools can help you improve the way you classify and manage information, which in turn enhances your ability to assess risk, govern and protect sensitive and business-critical data while efficiently responding to legal and regulatory obligations with intelligence and efficiency.

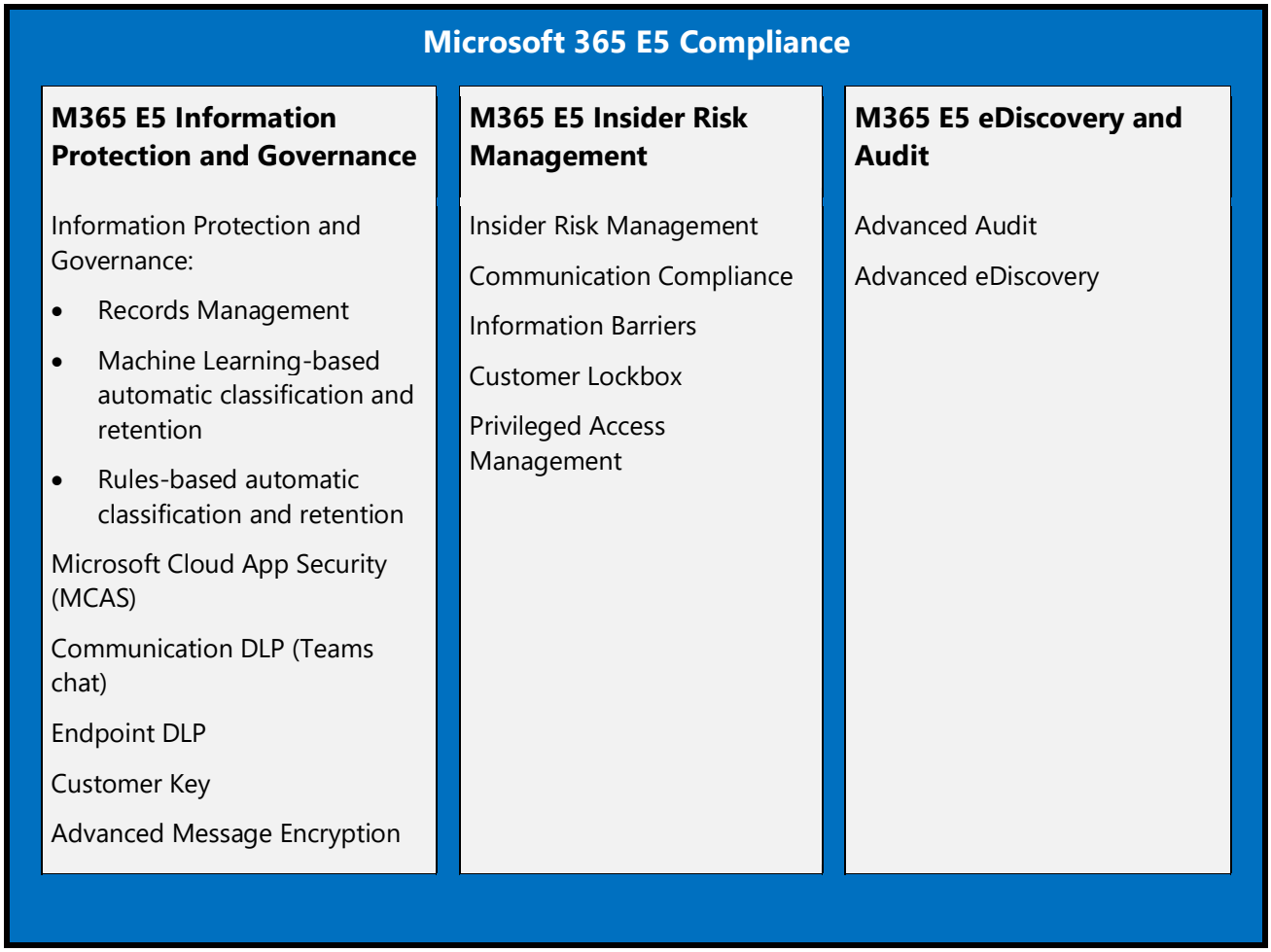
Agencies that are a part of the Whole of Government arrangement under the CUAMS2019 Supply of Microsoft product licences and licensing solutions[3] all have access to the Microsoft 365 E3 suite and the Microsoft 365 E5 security suite. Microsoft 365 E5 Compliance is available to add additional capabilities for Information Management and is further divided into three sections – Information Protection & Governance, Insider Risk Management, and eDiscovery & Audit – to ensure agencies have the maximum flexibility in choosing solutions that meet their specific requirements.

The E5 capabilities all build on what is currently available to agencies through the E3 licensing, and this document will highlight what could be done today as well as through additional investment.

1. https://www.wa.gov.au/government/publications/information-classification-policy
2. https://share.hsforms.com/12MvsJV43Tjm2Dsyw9Mn-_A2ge9t
3. https://www.wa.gov.au/government/cuas/supply-of-microsoft-product-licences-and-licensing-solutions-cuams2019

Licensing Information

The following image shows the components of the Microsoft 365 E5 Compliance bundle and the options available within it. For the purposes of this whitepaper, understand the components can be purchased through the mini-SKU, by adding E5 Compliance to existing E3 licensing, or by purchasing the entire Microsoft 365 E5 suite. This product set is current as of June 2021, however additional features will be added over time so please check the below links for the most up to date components of the compliance suite.



More information on licensing of the services is available from https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance.

You can also download a detailed comparison of SKUs from the above site in the following formats:
PDF: https://www.microsoft.com/download/details.aspx?id=103010
XLSX: https://www.microsoft.com/download/details.aspx?id=103006

Another resource, maintained by a Modern Work Specialist with Microsoft Australia but not an official Microsoft product, is the Microsoft 365 Maps site: https://m365maps.com.

Compliance requirements and solutions

The below table shows the technology mapping to a business requirement and whether they are included in the E3 or E5 compliance licensing. The solutions are described in more detail later in the document.

Business requirement	Associated features
Label and protect documents and e-mail messages	***Included in M365 E3:*** Information Protection (Office 365) Office 365 Message Encryption
	Included in M365 E5 Compliance: Rules-based Classification Advanced Message Encryption
Retain content for backup or records management purposes	***Included in M365 E3:*** Retention Policy Retention Labels
	Included in M365 E5 Compliance: Information Governance Records Management
Produce content for internal investigations and legal purposes	***Included in M365 E3:*** eDiscovery
	Included in M365 E5 Compliance: Advanced eDiscovery
Prevent accidental disclosure of sensitive information	***Included in M365 E3:*** Data Loss Prevention Intune Application Protection Policies
	Included in M365 E5 Compliance: Endpoint DLP Teams Data Loss Prevention *Microsoft Cloud App Security**
Discover and prevent inappropriate or malicious activity inside the agency	***Included in M365 E3:*** Alert Policies
	Included in M365 E5 Compliance: Communications Compliance Insider Risk Management Information Barriers
Provide greater visibility and control over your data	***Included in M365 E3:*** Alert Policies
	Included in M365 E5 Compliance: Advanced Audit Customer Lockbox Double Key Encryption Customer Key
Manage your organisation's regulatory compliance requirements	***Included in M365 E3 & E5:*** Compliance Manager

Note: Cloud App Security is also included in Microsoft 365 E5 Security

Common features

There are several features as part of the Microsoft 365 platform that support the compliance capabilities listed previously. Some of these may show on licensing diagrams in the E3 category but they underpin functionality available in both E3 and E5 capabilities.

Unified Audit Logging

The Microsoft 365 Compliance Centre (https://compliance.microsoft.com) hosts a search function for the Unified Audit Log, a central record of user and administrator activity within the Microsoft 365 environment. The audit log retains data for 90 days and captures events from several services including actions such as user access to documents, the use of eDiscovery searches, or the application of sensitivity labels. In addition to being available to search manually, you can configure alerts for specific events or access the entire audit log through the Office 365 Management Activity API. The audit log also performs a critical function in user behavioural analysis and is also surfaced through Cloud App Security.

More information on the unified audit log is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance.

Microsoft 365 E5 Compliance extends the retention period for the Unified Audit Log so you don't need to copy it to another location and captures additional activities over Microsoft 365 E3.

Sensitive Information Types

Sensitive information types are pattern-based classifiers that can detect information such as Medicare, passport, driver's license, credit card, or bank account numbers. Microsoft includes definitions for over 100 sensitive information types as part of Office 365, and organisations can create their own custom types based on patterns, keyword evidence, character proximity to evidence in a particular pattern, confidence levels, or even document fingerprints.

Sensitive information types have typically been used in the past for Data Loss Prevention and can be used with the E5 capabilities to automatically classify content for sensitivity or retention purposes. E5 customers can also create custom sensitive information types based on exact data matching.

More information on sensitive information types is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-learn-about.

Sensitive information types are available in Microsoft 365 E3, but with Microsoft 365 E5 Compliance licensing can be used to automatically assign a classification or retention label to a document or message.

Trainable Classifiers

A Microsoft 365 trainable classifier is a tool you can train to recognise various types of content by giving it samples to look at. Once trained, you can use it to identify items for the application of Office sensitivity labels, Communications compliance policies, and retention label policies.

This classification method is particularly well suited to content that isn't easily identified by either the manual or automated pattern matching methods and will identify an item based on what the item is, not by elements that

are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in classifying. The initial step is providing it examples of the data that you are looking to classify. Once it processes those, you test it by giving it a mix of both matching and non-matching examples. The classifier then makes predictions as to whether any given item falls into the category you're building. You then confirm its results, sorting out the true positives, true negatives, false positives, and false negatives to help increase the accuracy of its predictions. After you publish a trainable classifier, you can continue to train the model using a feedback process that is similar to the initial training.

There are two types of classifiers, pre-trained and custom.

Pre-trained classifiers are maintained by Microsoft and can be used immediately without training. At the time of writing Microsoft provide classifiers for resumes, source code, profanity, harassment, and threats.

Custom classifiers require significantly more work to build but are much better tailored to your agency's needs. Examples of classifiers you may wish to create include the following:

- Legal documents - such as attorney client privilege, closing sets, or statements of work.
- Strategic business documents - like press releases, merger and acquisition information, deals, business or marketing plans, intellectual property, patents, or design docs.
- Pricing information - like invoices, price quotes, work orders, or bidding documents.
- Financial information - such as organisational investments, quarterly or annual results.

Classifiers are a Microsoft 365 E5 or E5 Compliance feature. All users who will benefit from the feature must have one of these subscriptions to make use of them.

More information on trainable classifiers is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about.

Trainable classifiers require Microsoft 365 E5 Compliance licensing and use Artificial Intelligence and Machine Learning to identify your content based on a model. As with Sensitive Information Types, Trainable Classifiers can be used to automatically apply sensitivity and retention labels but can be more accurate than Sensitive Information Types due to the use of real content in the training.

Content Explorer and Activity Explorer

After you apply retention and sensitivity labels to your content you can use the Data classification section of the Microsoft 365 compliance centre to view summary information such as the top labels or sensitive information types in use. For more detailed information customers with E5 licensing can utilize the Content Explorer and Activity Explorer.

Content Explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your agency. You can then search or browse locations such as Exchange, SharePoint, and OneDrive to receive a listing of each item with the corresponding label. Additionally, users with the appropriate permissions can also view the content of the files directly through this interface, making it easy to review files for classification accuracy.

Activity Explorer allows you to see what is being done with your labelled content and provides a historical view of activities with over 30 filters including user, date, label, data type, and location. This information allows you to evaluate the effectiveness of data loss prevention controls through the review of actions such as downgrading a sensitivity label, printing messages, or copying items to a removable drive.

More information on Content Explorer is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer, and Activity Explorer from https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer.

Content Explorer and Activity Explorer, available with Microsoft 365 E5 Compliance licensing only, make it easy to see all the labelled and sensitive information throughout your Microsoft 365 tenant and track the activity associated with those items. These tools are intended to be used by information managers and offer a simple user interface.

Compliance scenarios

The following scenarios describe common compliance requirements and how they can be achieved using the compliance features in Microsoft 365.

Label documents and e-mail messages

Many organisations must comply with an information classification policy that defines how content should be identified and labelled. **Sensitivity labels** in Microsoft 365 can be used like a stamp to provide a visual marking on a document or message representing the level of sensitivity, and optionally to enforce protection settings based on that classification. The label itself is stored in clear text in the metadata of the file or message so it can be read by third-party applications and services, and roams with the content no matter where it might be stored.

Previously provided through Azure Information Protection, sensitivity labels are now a native capability of Microsoft 365 and can be created in the Microsoft 365 compliance centre. Agencies can create labels based on their classification scheme and make these available to users for selection directly within the Office applications for Windows, macOS, iOS, Android, and Office Online.

Optional protection settings allow content to be encrypted or marked by the label:

- Encryption prevents emails and documents from being accessed by unauthorized people. Labels can include specific permissions for all users in the tenant, members of defined security groups, or apply protection to recipients only, and these permissions can further restrict what actions users are allowed to perform with the content such as preventing printing or forwarding.
- Content marking applies watermarks, headers and footers to email, or documents as defined within the label.

Sensitivity labels are published to users or groups using label policies which can:

- Control which labels are available to users and groups; multiple policies can be used to provide a standard classification taxonomy to all users and additional labels for users in specific departments, job functions, or projects.
- Enforce a default label – content could be classified as Official by default but changed by the users, as necessary.
- Require a justification for changing a label – if a user selects a lower classification, they will be prompted for a reason that will be captured and displayed through the Activity Explorer.
- Require users to apply a label – whether a default label is provided or not, mandatory labelling ensures a label must be applied before users can save documents and send emails.

For agencies with Microsoft 365 E5 or E5 Compliance licensing, labels can also be applied automatically based on the content within a document or message. Sensitive information types can be used to identify information patterns such as Medicare, driver's license numbers, Passport numbers, bank accounts and credit card numbers, key words and phrases, or custom identifiers as defined by the agency. Exact data matching can be employed to detect exact values such as patient or customer names and addresses, and trainable classifiers can be taught to recognize types of content such as contracts or invoices.

For use outside of the core Microsoft 365 services:

- **Microsoft Cloud App Security** (included in the Government agreement as part of E5 Security) can be used to detect content at rest in other cloud services and apply sensitivity labels, or to intercept downloads from unmanaged devices and apply labels to ensure content cannot be saved in an unprotected state on devices not owned by the agency.
- **Azure Information Protection Scanner** can be used to discover and label content stored in on-premises file servers and SharePoint sites. Discovery of sensitive information and assignment of a specific label are both available as part of the Microsoft 365 E3 licensing available to all agencies, however using the automatic classification system to apply labels based on the content of individual files requires Microsoft 365 E5 or E5 Compliance.
- **Azure Information Protection Unified Labelling Client** provides a right-click option in File Explorer to apply labels to all file types and includes a viewer to display encrypted text, image, or PDF documents.
- **Azure Purview** (currently in preview) can discover, and label content stored in Azure Blob storage and database columns.
- Third-party applications and services can read labelling metadata and leverage the Microsoft Information Protection SDK to support labelling and encryption capabilities within their own platforms.

For more information on the use of sensitivity labels refer to https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels. We have also included an example of how a policy could be configured to label files and messages based on the Western Australian Government Information Classification Policy in Appendix B of this document.

While sensitivity labels typically provide the best user experience when sharing with people in your agency and your regular business partners, the limited client support and inability for recipients to remove the encryption and restrictions means **Office 365 Message Encryption** is better for communications with the general public. Put another way, OME, part of Microsoft 365 E3, is the better choice when you simply want to send something securely to someone outside your organization; what they do with the information after that is up to them. For example, use OME to securely share financial statements or patient records. Administrators define conditions under which to encrypt messages using Office 365 Message Encryption, for example a message to an external recipient containing sensitive information or a message including particular keywords, and the recipient either opens the message directly in Outlook or is redirected to the OME Portal where they can sign in with a Microsoft, Gmail or Yahoo account. Recipients can reply from the OME Portal or download attachments in an unencrypted format.

For additional control over the encryption experience, **Office 365 Advanced Message Encryption** in Microsoft 365 E5 Compliance allows the creation of multiple branding templates to tailor the experience based on the information being protected. In addition, administrators can force recipients to use the portal to open messages which ensures they see the custom branding and that access to messages can be revoked at any time. More information on Office 365 Message Encryption and Advanced Message Encryption is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide.

Use Sensitivity Labels to assign a classification to your documents and e-mails. Labels can optionally mark content with headers, footers and watermarks, or encrypt items and enforce restrictions to control who has access and what they can do. Microsoft 365 E3 contains everything you need to get started, and Microsoft 365 E5 Compliance provides automatic labelling. When you simply want to share information like statements or records securely with people outside the agency, consider using Office 365 Message Encryption and Advanced Message Encryption for a convenient, branded experience.

Retain content for backup or records management purposes

In a typical on-premises deployment you make regular copies of your data and keep them offsite in case you ever need to recover the information. In a cloud services deployment, the infrastructure is designed to be highly available and eliminate the chances of logical corruption through physical failure, so your backup needs will be different. Microsoft 365 includes the capability to preserve content in-place rather than through an external backup, and recovery can be performed either by users themselves or tenant administrators. Content can be retained for configurable periods of time and automatically deleted at the end of the retention period or held indefinitely even for users that have departed the agency and no longer have a licensed account.

Retention policies can be employed as part of the Microsoft 365 E3 licensing to preserve content at the container level. Policies could be applied to all files in SharePoint Online or OneDrive for Business sites, all items in users' Exchange Online mailboxes, or all channel messages within Microsoft Teams. If an item is deleted while protected by a retention policy, it will be preserved within a hidden location until the duration defined in the policy expires. This hold will apply even if the user's license is removed and their account deleted, meaning you do not need to pay for additional storage or take any specific actions to retain content as legally required when a user leaves the agency. Preserved content can be restored as part of the whole mailbox/site or discovered with Content Search and eDiscovery tools for selective export.

Microsoft recommends you consult with your Legal or HR teams to define how long you need to retain content and then set a standard retention policy to apply to all sites and users, otherwise you will only be able to recover content within the default limits of the services (ranging from 14-30 days). More information on retention policies is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/retention.

Users can recover their own deleted items from their mailbox within Outlook or Outlook on the Web; for more information on this see https://support.microsoft.com/en-us/office/recover-deleted-items-in-outlook-for-windows-49e81f3c-c8f4-4426-a0b9-c0fd751d48ce. Administrators can restore items for a user through a number of methods such as the Exchange Admin Centre or PowerShell, and more information is available from https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-user-mailboxes/recover-deleted-messages.

For items stored in OneDrive for Business or SharePoint Online there are several options for recovery depending on whether you need to restore deleted files, restore a particular version of a file, or restore a library to a particular point in time. These options are outlined at https://support.microsoft.com/en-us/office/restore-your-onedrive-fa231298-759d-41cf-bcd0-25ac53eb8a15.

While retention policies are a great solution for ensuring recovery akin to a backup solution, sometimes agencies will want to retain specific types of content for longer or shorter periods. Retention labels allow you to define retention or deletion schedules on individual documents or messages – for example, you might have a retention policy covering all sites and mailboxes with a 1-year retention period, and a label for Contracts that mandates 7-year retention. As part of Microsoft 365 E3 licensing retention labels can be applied manually within Outlook or SharePoint, or you could set a default retention label for specific document libraries.

Automatic application of retention labels based on the content of an item is possible with Microsoft 365 E5 Compliance licensing. Retention labels can be automatically applied based on a match to a Sensitive Information Type or a Trainable Classifier, as described earlier in this document. Labels can also be used to

declare items as a record or a regulatory record which places further restrictions on the item, logs additional activities, and provides proof of disposition when items are deleted at the end of the retention period. Retention labels are displayed in Content Explorer and Activity so records managers can easily discover where records are stored and monitor the associated activity. More information on Records Management is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management.

Microsoft partner **Engaged Squared** has created a whitepaper on **Modern Records and Information Management with Microsoft 365** in partnership with the Department of Local Government, Sport and Cultural Industries and the State Records Office of WA that can be downloaded from: https://share.hsforms.com/12MvsJV43Tjm2Dsyw9Mn-_A2ge9t.

Microsoft 365 E3 lets you keep all your users' files and e-mails, even after they've left the agency, based on your unique retention requirements. Users can self-recover in most cases, and administrators can recover content for users or as part of an investigation. E5 licensing adds the ability to automatically assign different retention labels depending on the content or to declare items an official record for added protection.

Produce content for internal investigations and legal purposes

Electronic Discovery, or eDiscovery is the process for identifying and delivering information that can be used as evidence in legal cases. Microsoft eDiscovery can search for content in Exchange Online mailboxes, Microsoft 365 Groups, Teams, SharePoint Online, Skype for Business conversations and Yammer teams. **Core eDiscovery** in Microsoft 365 E3 allows you to identify, hold and export content found within mailboxes and sites, while **Advanced eDiscovery** in Microsoft 365 E5 Compliance expands upon these capabilities – providing an end-to-end workflow to collect, preserve, review, analyse and export the required content for both internal and external investigations. It provides teams the functionality to manage custodians and the entire legal hold notification workflow to communicate with other custodians assigned to a case.

In some cases, it may be necessary to create a hold to preserve data that may be used in evidence; eDiscovery provides the ability to place a hold on data located in the Microsoft 365 platform, preserving this content until the location is removed from the hold, or until the hold is deleted. Further information can be found at https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery.

With the amount of data that agencies are creating it has become increasingly difficult to perform searches for specific content across the business environment, whether this be required for internal investigations of user content, or legal investigations from external parties. **Content Search** in Microsoft 365 E3 provides the capability to quickly find emails, documents and instant messaging conversations in Exchange mailboxes, OneDrive, Microsoft 365 Groups, and Microsoft Teams. It allows you to perform actions on this found content, such as exporting and downloading the results to a local device or delete the results of a search from a user's mailbox. Additional information for Content Search can be found at https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content.

Microsoft 365 E3 includes tools for searching for content and managing investigations through eDiscovery Cases. E5 adds Advanced eDiscovery with additional capabilities to identify relevant information and eliminate unnecessary details.

Prevent accidental disclosure of sensitive information

Increasingly organisations have the requirement to store and protect sensitive data, whether this be business critical data such as financial information or customer centric data, such as credit card numbers, health records or other Personal Identifiable Information (PII). As this data grows exponentially over time it becomes more difficult to monitor and protect this data from being exfiltrated, either maliciously or accidently. To protect this data and reduce risk, agencies need a way to prevent users from sharing it with people that should not have access to this data – this practice is referred to as Data Loss Prevention (DLP).

Microsoft DLP is a suite of technologies largely provided in Microsoft 365 E3 and covering Office DLP, Endpoint DLP, Teams DLP, on-premises DLP and MCAS DLP functionality and is implemented by defining and applying policies, allowing you to identify, protect and monitor sensitive items across Microsoft 365 Services, Office applications, Windows 10 Endpoints, non-Microsoft Cloud applications, on-premises file shares, and on-premises SharePoint. Policies are created to provide functionality to monitor the activities that end users take on data both in rest and in transit, and take preventative actions, such as blocking the sharing of the sensitive data. These activities are all recorded to the Microsoft 365 Audit log and routed through to Activity Explorer. If the policy has been created to generate an alert once an action occurs, these will appear in the DLP management dashboard. More information about Microsoft DLP can be found at https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp.

Sensitive data does not only exist within the cloud, and commonly exists in some form on the user's endpoint device. **Endpoint DLP** in Microsoft 365 E5 Compliance extends the activity monitoring and capabilities to sensitive items located on Windows 10 devices. Once these devices are onboarded to the solution, activity related to sensitive items on device are made visible through Activity Explorer and further protective actions can be enforced via DLP policies. These policies can be configured specifically for endpoint protection, such as restricting access to uploading by unallowed browsers, or auditing the copying of data across a remote session. Additional information for Endpoint DLP can be found at https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about.

With agencies adopting more collaboration tools to facilitate remote work, it has become increasing important to monitor and protect information across those tools. **Teams DLP** in Microsoft 365 E5 Compliance can be used to define policies that monitor and protect sensitive data in Microsoft Teams conversations and documents. A DLP policy can be used to detect when sensitive information is shared in a channel that has guest users and delete this sensitive data within seconds. Policy tips can be created to assist in the education of users and advise when and why a DLP policy was triggered. Additional information or Teams DLP can be found at Data loss prevention and Microsoft Teams - Microsoft 365 Compliance | Microsoft Docs

Microsoft Cloud Application Security (MCAS) can be used to extend these DLP capabilities to non-Microsoft Cloud applications **(Preview)**. With this solution, DLP policies can be used to monitor and detect when sensitive data is used and shared across non-Microsoft cloud applications. To use DLP policies for specific non-Microsoft cloud applications, the app must be connected to MCAS, once connected you can monitor and protect sensitive data that are shared through these applications. File policies allow for the control of actions that you can execute within MCAS once a policy match has been detected, whilst DLP policies allow for additional control over non-Microsoft cloud applications themselves. More information for MCAS can be found at https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-use-policies-non-microsoft-cloud-apps

Agencies typically have a large on-premises infrastructure that may contain sensitive data, this can range from legacy infrastructure to systems that are being prepared for the migration to the cloud. In this instance the **Microsoft 365 Data Loss Prevention on-premises Scanner (Preview)** can be utilized. The scanner crawls on-premises file shares and SharePoint document libraries and folders for sensitive data that can pose a risk of a compliance policy violation to provide additional visibility and control to manage sensitive data on-premises. It detects sensitive information using the built-in sensitive information types, custom information types, defined sensitivity labels, or different file properties. This information is then made visible in the Activity Monitor while protective actions and enforced via DLP policies. The on-premises DLP scanner relies on a full implementation of

the Azure Information Protection scanner to monitor, label, and protect sensitive data. Additional information can be found at https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-on-premises-scanner-learn

Data Loss Prevention included in Microsoft 365 E3 covers e-mail and files shared from OneDrive for Business and SharePoint Online. For greater visibility and control, Microsoft 365 E5 adds DLP for client devices, on-premises servers, cloud locations, and Teams chats. User education is a critical element across the solution, guiding people to use appropriate solutions for storing and sharing information.

Discover and prevent inappropriate or malicious activity inside the agency

Managing and minimizing risk starts with understanding what risks the agency may face in the modern workplace. Some may be driven by external events that are outside of the agency's control, whilst some are driven by internal events and user behaviour that can be controlled and avoided. These may come in the form of unethical, inappropriate, and malicious activities within your organisation, or can simply be the result of an inadvertent action such as the accidental sharing of sensitive information.

Microsoft 365 provides the capability to detect, investigate and act on malicious and inadvertent internal activities within your organisation. With **Insider Risk**, you define the types of risks that you want to identify and detect such as potential IP theft or intentional/unidentical leaks of information with the additional capability of escalating cases into Advanced eDiscovery if required. Utilizing Insider Risk Analytics (Currently in Preview) enhances these capabilities without the need to configure additional risk policies and enables you to evaluate potential insider risks within your organisation to provide a high-level view of the activities that your users are taking as well as any developing trends. More information is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management.

Communication Compliance helps to minimize communication risks by capturing and acting on inappropriate messages within your organisation using both custom and pre-defined policies allow you to scan both internal and external communications for policy matches within email, Microsoft Teams, Yammer, and third-party communications to allow the agency to take appropriate actions to ensure that you remain compliant with message standards or corporate policy. Once a policy detects a violation, remediation workflows can be utilized to take automated action, including the option to escalate messages to a reviewer, or to email the user that had the policy violation. Additional information is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance.

Microsoft cloud includes many powerful communication and collaboration capabilities, but suppose you need to restrict these communications between groups to avoid conflicts of interest in your agency – such as teams that work with highly confidential information? **Information Barriers** provides the capability to restrict information across Microsoft Teams, SharePoint Online and OneDrive for Business by defining policies to either allow or deny communications between groups. These policies can prevent users from calling or communicating with users outside of the policy, or to communicate only with a subset of user groups as defined. More information is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers.

Stepping beyond the basics with Data Loss Prevention controls, these Microsoft 365 E5 Compliance capabilities monitor for inappropriate usage by business users and block or alert on specific activities.

Provide greater visibility and control over your data

Microsoft 365 provides a record of all activity performed by users and admins in the unified audit log for the tenant, and this information is leveraged by many of the features described previously in this document. **Basic Audit** is enabled by default and more information is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/auditing-solutions-overview.

The **Office 365 Management Activity API** enables exporting of audit log details for external retention or connection to a Security Information and Event Management (SIEM) solution such as Azure Sentinel. For those without a SIEM, **Office 365 alert policies** would allow you to raise alerts based on activity recorded in the tenant and are available as part of Microsoft 365 E3. Alert policies allow you to define activity you wish to know about, for example malware detected in SharePoint and OneDrive or the creation of an anonymous sharing link, assign a severity, and configure how often to notify you. More information on alert policies is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies.

Microsoft Cloud App Security gives you visibility into all the activities from your connected apps and provides a much richer investigative experience for the Microsoft 365 audit log. In addition, Cloud App Security can provide advanced alerts through correlation of activities and anomaly detection policies, as well as detailed information on cloud application usage and data loss prevention events. Cloud App Security is available as part of Microsoft 365 E5 Compliance; however, it is also included in Microsoft 365 E5 Security and is therefore available to most Western Australian Government agencies today. More information on using Cloud App Security to investigate activities is available from https://docs.microsoft.com/en-us/cloud-app-security/activity-filters, and information on alert management is available from https://docs.microsoft.com/en-us/cloud-app-security/managing-alerts.

While Basic Audit as part of Microsoft 365 E3 provides for 90-day audit log retention, **Advanced Audit** in Microsoft 365 E5 Compliance allows for retention up to one year (or 10 years with an add-on license). In addition to long-term retention Advanced Audit allows the recording of high-value events that may be useful in forensic or compliance investigations, for example when messages were accessed, replied to, or forwarded, or what users searched for in Exchange or SharePoint Online. More information on Advanced Audit is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit.

For highly regulated customers or those with extremely sensitive data, Microsoft offers a number of capabilities in Microsoft 365 E5 Compliance that allow you to enforce strict control over access to information. While Microsoft engineers do not have access to your data by default, in limited cases it may be necessary to obtain customer data access to fix a support issue and the required permissions would be granted for a limited time through an approval workflow, the details of which you would see in the ticket history and the audit log. With **Customer Lockbox**, nominated administrators have the final say in the approval workflow and no access to data will be permitted without your explicit consent. This has been used by other customers in the past where regulatory requirements mandate access by Australian citizens only; while this may mean the support request cannot be completed, the compliance requirement can still be met. More information on Customer Lockbox is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests.

Office 365 utilizes advanced encryption to protect content at rest in services such as Exchange Online and SharePoint Online. For customers with regulatory requirements to control encryption keys Microsoft offers **Service Encryption with Customer Key**, which adds an additional layer of encryption using keys controlled by the customer. Note that this does not affect access to your data by Microsoft support personnel as the encryption is transparent to the services, however it ensures the content is not accessible if the keys are ever revoked (in other words, this capability is effectively a "kill switch"). More information on Customer Key is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-key-overview.

Finally, for customers with extremely sensitive content, **Double Key Encryption** uses two keys to encrypt files, one stored by Microsoft in Azure and the other provided by the customer. Both keys are needed to decrypt files, and since Microsoft would not have access to your key this ensures only those users specifically authorized by the customer have access to the content. Note that this has a considerable impact on the functionality the

services can offer related to those files, so this should only be used when necessary. The following features are not available with Double Key Encryption:

- Transport rules including anti-malware and spam that require visibility into the attachment
- Microsoft Delve
- eDiscovery
- Content search and indexing
- Office Web Apps including co-authoring functionality

More information on Double Key Encryption is available from https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption.

Microsoft 365 E3 ensures you have *visibility* into access to your data through the unified audit log. With Microsoft 365 E5 Compliance, you have *control*. From approval of Microsoft access to your data to control over encryption used in the tenant, E5 Compliance helps you meet the strictest regulatory and information protection requirements.

Manage your organisation's regulatory compliance requirements

The Microsoft 365 Compliance Centre includes the new **Compliance Manager**, an enhancement to the version in the Service Trust Portal and replacement for the Compliance Score preview. Compliance Manager is an end-to-end compliance management solution and helps simplify compliance and reduce risk by providing:

- Pre-built assessments for common industry and regional standards and regulations, or custom assessments to meet your unique compliance needs.
- Workflow capabilities to help you efficiently complete your risk assessments through a single tool.
- Detailed step-by-step guidance on suggested improvement actions to help you comply with the standards and regulations that are most relevant for your agency. For actions that are managed by Microsoft, you'll see implementation details and audit results.
- A risk-based compliance score to help you understand your compliance posture by measuring your progress in completing improvement actions.

For agencies with Microsoft 365 E3 licensing Compliance Manager includes the Data Protection Baseline assessment, however Microsoft 365 E5 Compliance adds assessments for GDPR, NIST 800-53, and ISO 27001. Customers with Microsoft 365 E5 can use custom assessments and premium assessment templates, which will be available to purchase as an add-on in the second half of CY21. There are currently over 300 premium templates available, including the Australian Privacy Act, IRAP v3, APRA CPS, Australian Energy Sector Cyber Security Framework, and the ASD Essential 8. For the full list of templates see https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-list, and for more information on Compliance Manager see https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager.

Compliance Manager is included with all Microsoft 365 subscriptions but the assessment templates available vary depending on your licensing. Premium assessment templates are available for Australian regulations and standards and will be available to purchase in the second half of CY21.

Summary

Microsoft 365 includes extensive compliance capabilities to meet the needs of our government customers, the most common of which have been described in this whitepaper. While the E5 Compliance solutions offer clear value in delivering a complete solution, don't overlook the capabilities you already own with Microsoft 365 E3 – get started today manually labelling content for sensitivity or retention, and use the built-in DLP capabilities to prevent accidental sharing through Exchange Online, SharePoint Online, and OneDrive for Business.

Microsoft provides education and support through our ongoing engagement with the Government of Western Australia and can offer direct assistance through Microsoft FastTrack and Premier or Unified Services Agreements.

Additionally, Microsoft has a rich partner community that can help extend our capabilities or assist with implementation and customized solutions. As an example, **Engage Squared** has written a whitepaper on **Modern Records and Information Management with Microsoft 365** that goes into more detail than this overview document. Written in partnership with the Department of Local Government, Sport and Cultural Industries and the State Records Office of WA, this whitepaper offers detailed information on migrating to a native Microsoft Records Management solution. The Engage Squared whitepaper can be requested from https://share.hsforms.com/12MvsJV43Tjm2Dsyw9Mn-_A2ge9t.

FastTrack for Microsoft 365 is included in eligible subscriptions and available at no additional cost. FastTrack provides remote assistance through a combination of tools, published documentation, and best practices to help you successfully enable services and take full advantage of your purchase. More information on the workload scenarios supported by FastTrack is available from https://docs.microsoft.com/en-us/fasttrack/products-and-capabilities

For more information on any of the capabilities described in this whitepaper please contact your Microsoft Account Team using the details at the beginning of the document.

Appendices

Appendix A: Microsoft Training and Certification

Microsoft Enterprise Agreement Yammer Group
Administered by the WA Department of Finance, this invitation-only group is available to approved agencies and provides a means to communicate between Microsoft and agencies in the Whole of Government agreement. The group hosts announcements on training opportunities and recordings of previous sessions.

Microsoft Snackable Series for WA Government
The Microsoft Snackable Series offers short webinars delivered through Microsoft Teams by Microsoft experts on both technical and non-technical subjects. These sessions cover popular topics and provide overviews, updates, and tips. Attendance is open to all agencies under the Whole of Government agreement and recordings are posted to the Yammer group.

Microsoft Compliance Customer Experience Engineering Webinars
http://aka.ms/mipc/webinars

Deep-dive webinars conducted by the Compliance CxE team on new and upcoming features. Presentations are recorded and decks and videos are available for all past sessions.

Microsoft Certified: Security, Compliance, and Identity Fundamentals
https://docs.microsoft.com/en-us/learn/certifications/security-compliance-and-identity-fundamentals/

This certification is intended for those looking to familiarize themselves with the fundamentals of security, compliance and identify across cloud-based and related Microsoft services. This exam and associated Learning Path will help you understand the solutions available in E3 and E5 licensing and when you would use each capability. This is a great place to start for IT Professionals and business users alike.

Microsoft Certified: Security Operations Analyst Associate
https://docs.microsoft.com/en-us/learn/certifications/security-operations-analyst/

This certification is intended for people responsible for securing information technology systems for the organisation. The exam and learning path are focused on investigating, responding to and hunting for threats using Microsoft Azure Sentinel, Microsoft Defender, Microsoft 365 Defender, and other third-party security products.

Microsoft Certified: Identity and Access Administrator Associate
https://docs.microsoft.com/en-us/learn/certifications/identity-and-access-administrator/

This certification is intended for people responsible for implementing, and operating an organisation's identity and access management systems by using Azure AD. The exam and learning path are focused on Azure AD capabilities including general administration and implementation of hybrid identity, Azure AD Identity Protection, and Identity Governance.

Microsoft Certified: Information Protection Administrator Associate
https://docs.microsoft.com/en-us/learn/certifications/information-protection-administrator/

This certification is intended for people responsible for planning and implementing controls to meet organisational compliance needs. The exam and learning path are specifically focused on Microsoft Information Protection, Data Loss Prevention, and Information Governance.

Appendix B: Sample sensitivity labelling based on the WA Government Information Classification Policy

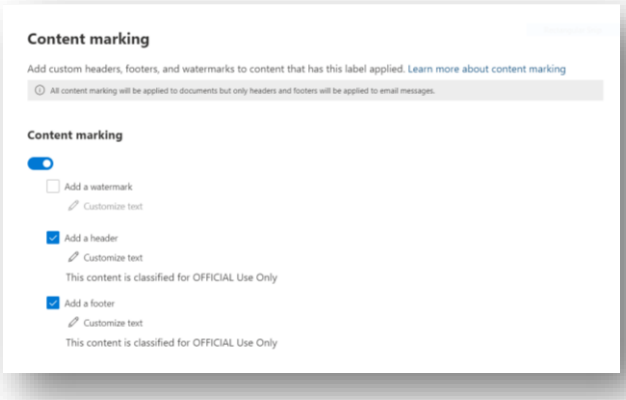
Note: this information is provided for consideration only and should not be taken as official Microsoft guidance for meeting compliance with WA Government requirements. For assistance with strategy and implementation please contact Microsoft or one of our partners.

The Western Australian Government Information Classification Policy, Version 2 (https://www.wa.gov.au/government/publications/information-classification-policy) requires agencies to label all new content based on the following classifications:

- **UNOFFICIAL**
- **OFFICIAL**
- **OFFICIAL: Sensitive**

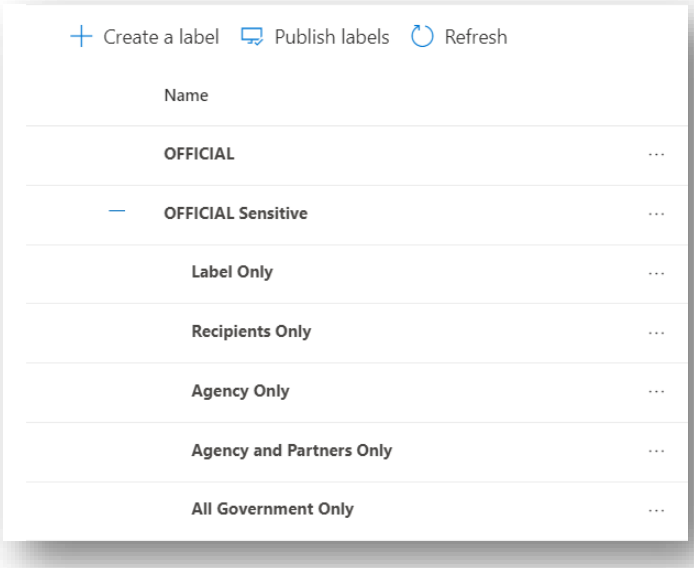
Other than a reference to the Digital Security Policy and information on the handling of classified content, the policy does not provide any guidance around protection of content through measures such as Information Rights Management. Microsoft Information Protection can both label the content as required by the policy and enforce optional protections, limiting access to specific agencies or security groups and restricting what actions authorized users may perform.

Implementing the Information Classification Policy in Microsoft Information Protection is relatively simple and at a minimum would consist of creating three labels, one for each classification. Labels could be set to apply headers and footers to documents or e-mails, and the presence of the label could be used to prepend the email subject line.



Given the broad use of these three labels applying anything beyond basic content marking would be untenable, so as an alternative OFFICIAL: Sensitive and potentially OFFICIAL could instead be implemented as parent labels with sub-labels configured to apply specific restrictions.

Consider the following example using OFFICIAL: Sensitive:



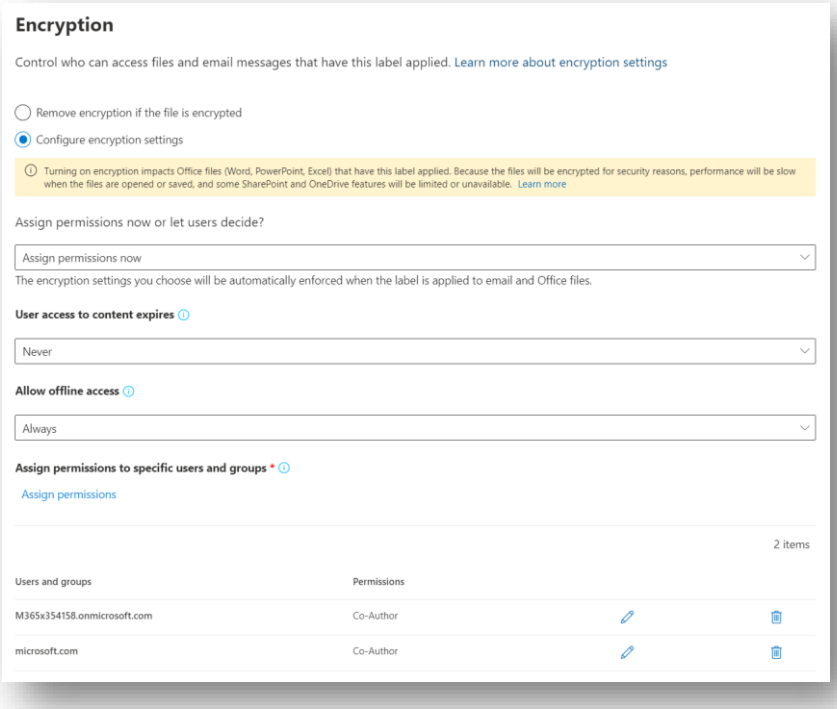
In this policy, **OFFICIAL Sensitive** could not be applied on its own and one of the sub-labels would need to be selected. **Label Only** could do exactly that, simply apply a label as in the prior screenshot for the OFFICIAL label. This would apply when you want to label the content, as is likely standard practice today, but not enforce any restrictions on the document or message itself.

Recipients Only could allow users to define custom permissions when creating a document or to prevent anyone other than the original recipients of an e-mail from being able to open it. This would also prevent recipients from forwarding, copying, or printing e-mail messages.

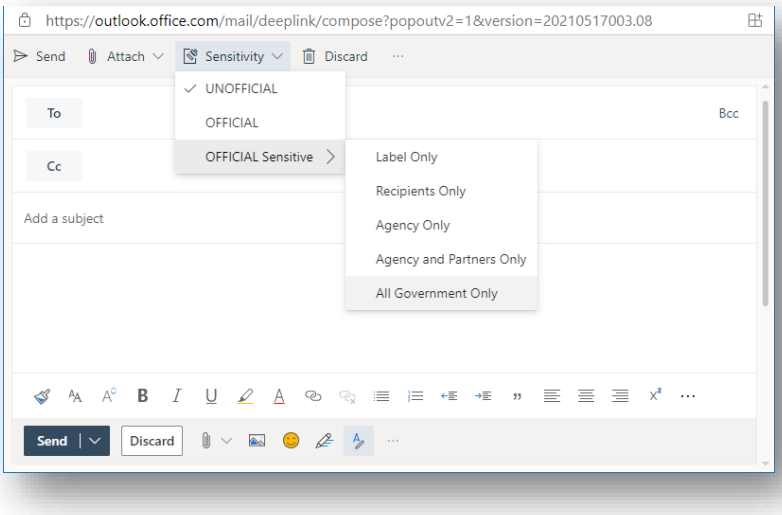
Agency Only could restrict documents and e-mail messages to members of the agency's tenant only, or to a specific security group if distinction between full-time employees and volunteers/contractors is required (for example). Users could have full control over documents and messages, and therefore print and share internally as necessary, but anyone not signed in with an agency user ID would be prompted for credentials when attempting to open content and would therefore be unable to decrypt the item to access the information.

Agency and Partners Only could be used where multiple agencies need to collaborate. Since all agencies are using Microsoft 365 the appropriate e-mail domains could be added to the policy and restrictions would be enforced through the Azure AD Rights Management Service.

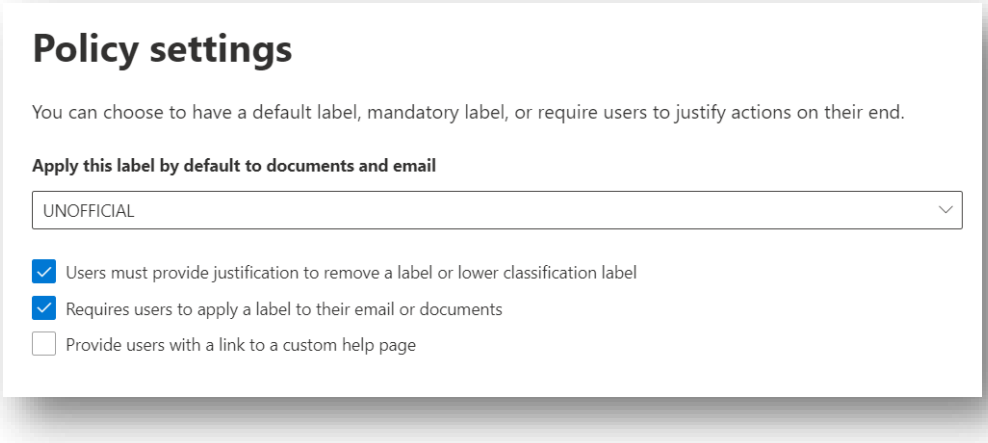
All Government Only could build on the previous label and include the domains for all government agencies. With this policy in place, one agency could create a document or e-mail message that could be opened only by people with a valid WA Government user account. To ensure consistency between agencies the definition of this label should be centrally owned and potentially created/updated only through a PowerShell script.



Implemented together, the user experience when assigning a label to a document or e-mail would look like this screenshot from Outlook on the Web:



The capabilities described are all part of the Microsoft 365 E3 licensing available to all Western Australian Government agencies and could be implemented today with minimal effort. To begin with, labels could be applied manually by users when deemed necessary, but the product includes the ability to define a default classification or require users to select a classification before they can save a document or send an e-mail.



Automatic or recommended labelling provided through Microsoft 365 E5 Compliance could be employed when dealing with items containing definable sensitive information, but everything needed to get started with labelling and protection is included in the government agreement today.