Microsoft

Microsoft 365 Guidance for UK Government

Information Protection

Prepared for UK Government

7/12/2023

Version 1.0 Final

Prepared by

Microsoft UK

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

Table of Contents

1 Blueprint Summary

Following the recent update to the Government Security Classification Policy (GSCP) Microsoft have partnered with Government Security Group, the Central Digital and Data Office and the National Cyber Security Centre (NCSC) to provide configuration guidance for those wishing to implement the OFFICIAL tier of the GSCP using Microsoft Purview Information Protection (MPIP), available as part of Microsoft 365. The guidance assists those wishing to classify and protect files, control who can access them, and allow greater control when sharing information between departments, partner organisations, and customers.

A spokesman from the Government Security Group said," The Government Security Classifications policy (GSCP) sets out the administrative system used by HM Government (HMG) and our partners to appropriately protect information and data assets against prevalent threat actors. The GSCP was updated in 2023.

This gave us a significant opportunity in UK government to modernise and standardise how organisations apply technical controls in line with security classifications. Microsoft 365 is widely used across UK government, so we partnered directly with Microsoft to define a standard approach to applying sensitivity labels and data loss prevention features of Microsoft 365 in line with the GSCP.

The resulting technical guidance provide a baseline from which organisations can select the most relevant elements and tailor them for their specific use cases. Our objective is that this will be an enabler for the GSCP and that it will also create a better user experience for civil servants and our partners."

1.1 Intended Audience

Technical staff responsible for the configuration and deployment of Microsoft 365 (M365) services across UK government departments.

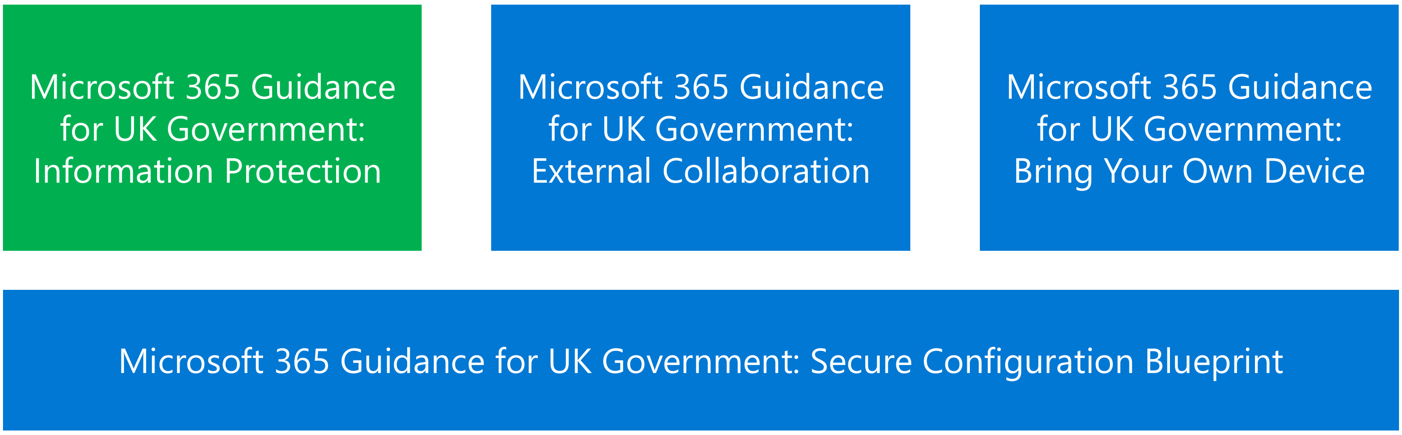
Security staff responsible for securing and monitoring information sharing.

1.2 Document Purpose

In partnership with the National Cyber Security Centre, Microsoft produced Microsoft 365 Guidance for UK Government: Secure Configuration Blueprint guidance for UK Public Sector on how to configure their Microsoft 365 tenants for use at the OFFICIAL tier (including with the OFFICIAL-SENSITIVE marking).

This document builds on top of the "Office 365 UK Blueprint – Secure Configuration Alignment". It describes how to configure the Microsoft Purview Information Protection capabilities available in Microsoft 365. This provides a way to classify and protect files, control who can access them and allow greater sharing of information between departments, partner organisations, and customers.

1.3 How to use this document



Microsoft 365 Guidance for UK Government: Information Protection

Microsoft 365 Guidance for UK Government: External Collaboration

Microsoft 365 Guidance for UK Government: Bring Your Own Device

Microsoft 365 Guidance for UK Government: Secure Configuration Blueprint

Figure 1: Relationship with other NCSC and Microsoft guidance

It draws on broad experience across UK government, industry and incorporates existing best practice that is published by the Microsoft.

The Microsoft 365 Guidance for UK Government: Information Protection is assumed to be adopted alongside other key technical guides for government organizations working in Microsoft 365:

1. The Microsoft 365 Guidance for UK Government: Secure Configuration Blueprintwas produced by Microsoft and the NCSC and updated in June 2023. It should be implemented as a secure foundation on which to adopt this guidance.
2. The Microsoft 365 Guidance for UK Government: External Collaboration was produced by the NCSC and Microsoft and updated in June 2023. It provides configuration guidance to allow easier and more consistent collaboration between government organisations using Microsoft 365 services.
3. The Microsoft 365 Guidance for UK Government: Bring Your Own Device was produced by the NCSC and Microsoft updated in June 2023. It provides configuration guidance to allow personally owned mobile devices to connect to Microsoft 365 using Mobile Application Management policies for unenrolled devices in Microsoft Intune.

This document contains four main sections:

- Section 3 Information Protection principles describes the overarching principles which should be observed regardless of the implementation phase.
- Section 4 Labelling taxonomy covers the following centrally defined label elements of the GSCP at the OFFICIAL tier.
- Section 5 Enablement phases – crawl, walk, run in which the capabilities are introduced in stages, firstly focusing on elements which cause minimal disruption, such as manual labels without protection, adding basic protection elements in a later stage (e.g. DLP controls to prevent highly confidential items from being accidentally sent outside, or encryption with very broad rights applied), and finally adding more restrictive permissions and tighter controls once you are confident in the use of the technology.
- Section 6 Enhanced capabilities the features and capabilities described in this section require Microsoft 365 E5 or Microsoft 365 E5 Compliance and build upon the previously implemented capabilities to allow further automation of labelling, more granular control for web sessions, and more sophisticated DLP capability for endpoints.

> ### Important
>
> This guidance has been written as a starting point and organisations should consider how they may wish to supplement it with additional controls, as appropriate for your environment and risk appetite.

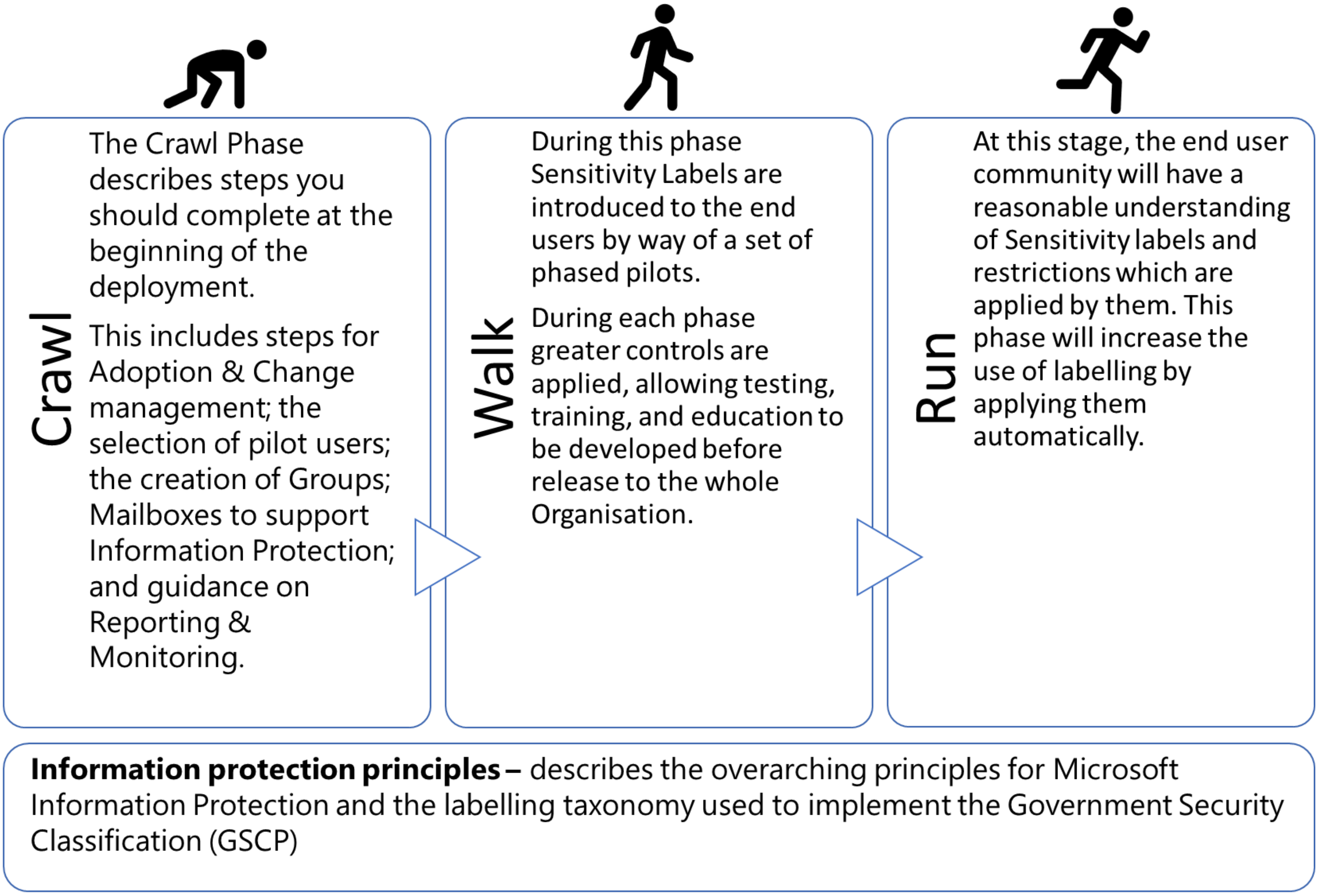
> The items described in this document are intended to explain the recommended security controls and provide links to additional configuration guidance. The intent is to help you understand how the features and capabilities in Microsoft 365 can be used, and to ensure that a common bar has been achieved for your tenant.

2 Blueprint Overview

This blueprint guidance has been structured to follow a Microsoft recommended three phased approach for implementation: ‘Crawl, Walk, and Run’. This differs from the ‘Good/Better/Best’ pattern that is used in the Microsoft 365 Guidance for UK Government: Secure Configuration Blueprint.

Adopting sensitivity labelling is a complex task that experience shows is best broken down into a phased implementation. With the ‘Crawl, Walk, Run’ approach, changes can be introduced in waves across your organisation, focusing on small sets of users first and then expanding to broader audiences. This will allow you to deploy quickly whilst minimising disruption, and help you get a baseline of user behaviour before introducing tighter restrictions. It will help you identify early potential conflicts or compatibility issues between different tools, so you can address them before they have significant impact.

The guidance is made up of the following major sections:



The Crawl Phase describes steps you should complete at the beginning of the deployment.

This includes steps for Adoption & Change management; the selection of pilot users; the creation of Groups; Mailboxes to support Information Protection; and guidance on Reporting & Monitoring.

During this phase Sensitivity Labels are introduced to the end users by way of a set of phased pilots.

During each phase greater controls are applied, allowing testing, training, and education to be developed before release to the whole Organisation.

At this stage, the end user community will have a reasonable understanding of Sensitivity labels and restrictions which are applied by them. This phase will increase the use of labelling by applying them automatically.

Information protection principles – describes the overarching principles for Microsoft Information Protection and the labelling taxonomy used to implement the Government Security Classification (GSCP)

Figure 2 - Crawl-Walk-Run phases

> Important
>
> While implementing the Microsoft Purview Information Protection configurations in this guidance, departments should be prepared that a concerted effort needs to be afforded for cultural and

> organisational change, and appropriate training and education resources made available to your user community. Sample training materials can be downloaded from [here](#).

The components that make up the Microsoft Purview Information Protection Blueprint guidance are illustrated in Figure 3

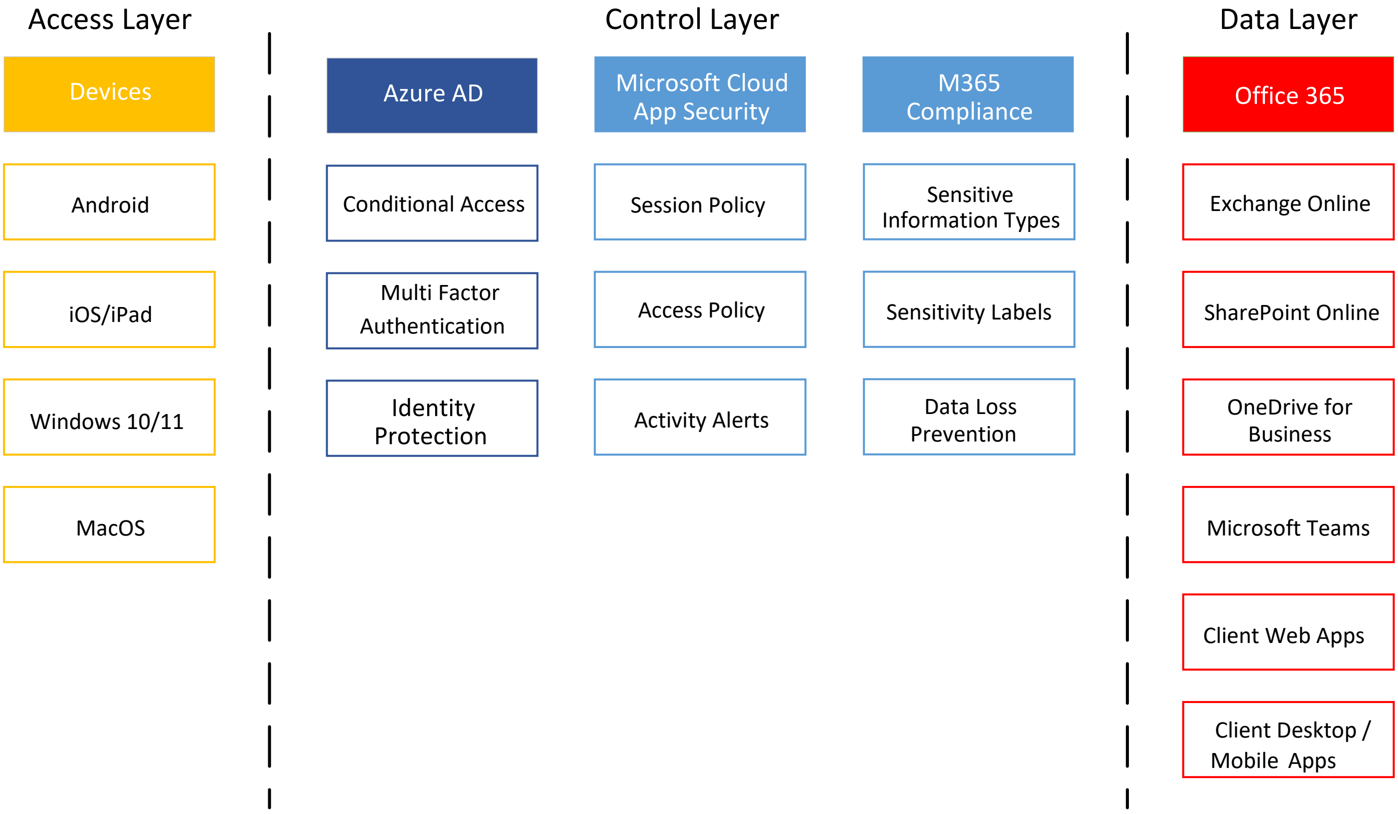


Figure 3: Microsoft Purview Information Protection Blueprint components

The guidance covers three primary configuration patterns that have been identified as meeting the requirement to allow users to apply a label to corporate data and have the appropriate controls apply to that data, these are:

- Microsoft 365 applications on your managed devices/PC, Mac, Android, and iOS.
- Microsoft 365 applications on verified managed guest devices.
- Microsoft 365 Web access on unverified guest devices.

The framework has been designed to be deployed to all users in the organisation, with the expectation that this will provide sufficient coverage for 90% or more of the typical day-to-day business operations. However, it is possible to set up additional controls that can be targeted at sub-sections of the organisation for very specific purposes. For example, there may be a need for the legal department to have a specific sensitivity label that applies encryption so only authorised legal personnel can work with that data. This can be achieved, but caution should be applied to ensure these are only used in exceptional circumstances. It is very easy to introduce 'label sprawl', whereby labels are created too frequently, which quickly becomes unwieldy and difficult to manage.

2.1 Supporting information

The following list provides a set of supporting information that this guidance on assumes has been followed:

1. Microsoft 365 has been assessed against the recommendations for your organisations licensing level in the Microsoft 365 Guidance for UK Government: Secure Configuration Blueprint. Unless Cross-tenant Access settings is used it is recommended that guest devices use web apps to access content (refer to note below).
2. Cross-Government Collaboration – Technical Configuration recommendations have been assessed and are being implemented in your organisation.
3. Devices managed by your organisation that are used to connect to the Microsoft 365 services have been configured in accordance with the NCSC's Platform-specific guidance for mobile and PC devices.
4. Only allow approved apps on managed mobile devices.
5. Require MFA with Compliant or Hybrid Azure AD Joined devices to access Microsoft 365 services.

BYOD can be included in scope if organisation risk appetite allows it. Refer to the BYOD guidance for more info:

> Important
>
> This document intentionally does not cover controls available to you when devices are personal unmanaged Bring Your Own Device (BYOD) or guest devices; it focuses on the controls that are available for Microsoft Intune as managed devices or Microsoft Intune and Configuration Manager co-managed devices.
>
> For BYOD refer to Microsoft 365 Guidance for UK Government: Bring Your Own Device guidance.
>
> This document intentionally does not cover controls available that allow secure collaboration between departments. It has been developed to work in conjunction with the configuration guidance described in Microsoft 365 Guidance for UK Government: External Collaboration and the supporting Technical Implementation guide.

- Table 1 illustrates the controls which are implemented as part of this blueprint guidance, the suggested phase for implementation, and a mapping to the sensitivity labelling related recommendations in the Microsoft 365 Guidance for UK Government: Secure Configuration Blueprint ('Good/Better/Best') levels for comparison to maturity of that guide.

Table 1 - Purview components

	Microsoft 365 Licence			Phase				Microsoft 365 SCB		
	E3	E5 Security	E5 Compliance	Crawl	Walk	Run	Enhanced Capabilities	Good	Better	Best
Manual, default sensitivity labelling in Microsoft 365	✓				✓			✓		
Mandatory labelling	✓					✓			✓	
Sensitivity labelling for containers in Microsoft 365	✓				✓			✓		

	Microsoft 365 Licence			Phase				Microsoft 365 SCB		
	E3	E5 Security	E5 Compliance	Crawl	Walk	Run	Enhanced Capabilities	Good	Better	Best
O365 Data Loss Prevention (DLP) for emails & files	✓				✓			✓		
Automatic sensitivity labelling in Microsoft 365 apps			✓				✓			✓
Automatic sensitivity labels in Exchange, SharePoint, and OneDrive			✓				✓			✓
Sensitivity labels based on advanced classification (ML, EDM)			✓				✓			✓
Endpoint DLP			✓				✓			✓

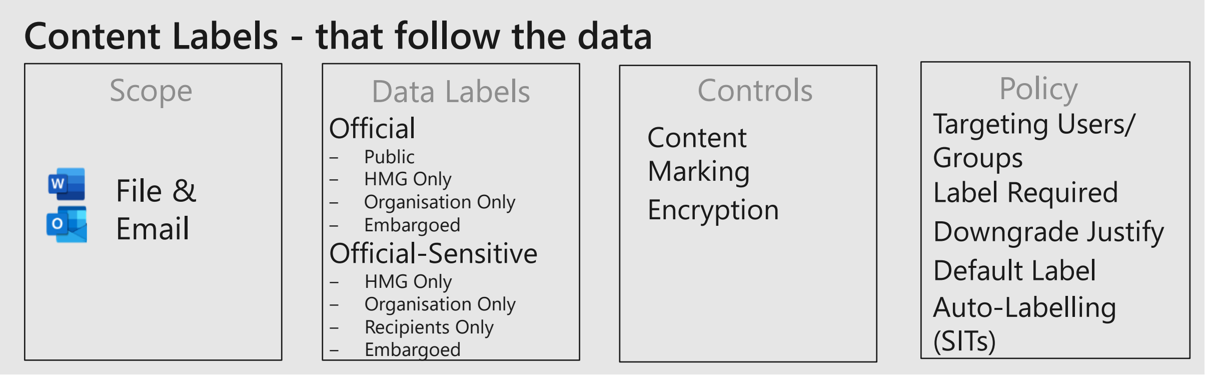
2.2 Outcome based approach

The visual indication provided with sensitivity labels is one small, but important part of the possible capability that sensitivity labels can provide.

This guidance looks to provide ‘outcomes-based’ approach which aims to reduce the likelihood of accidental data loss or oversharing. It utilises the features available in Microsoft Purview Information Protection to further protect access to documents, based on the label that is selected, and then leveraging additional technical controls to supplement the visual markings as appropriate (e.g., OFFICIAL–FOR PUBLIC RELEASE label does not leverage additional technical controls for protection). The sensitivity labels are broken down into two distinct areas:

Content Labels

Content labelling applies the label directly to documents and emails. This stamps the data with label metadata which is maintained wherever the data resides.



Content Labels - that follow the data

Scope

File & Email

Data Labels

Official
- Public
- HMG Only
- Organisation Only
- Embargoed

Official-Sensitive
- HMG Only
- Organisation Only
- Recipients Only
- Embargoed

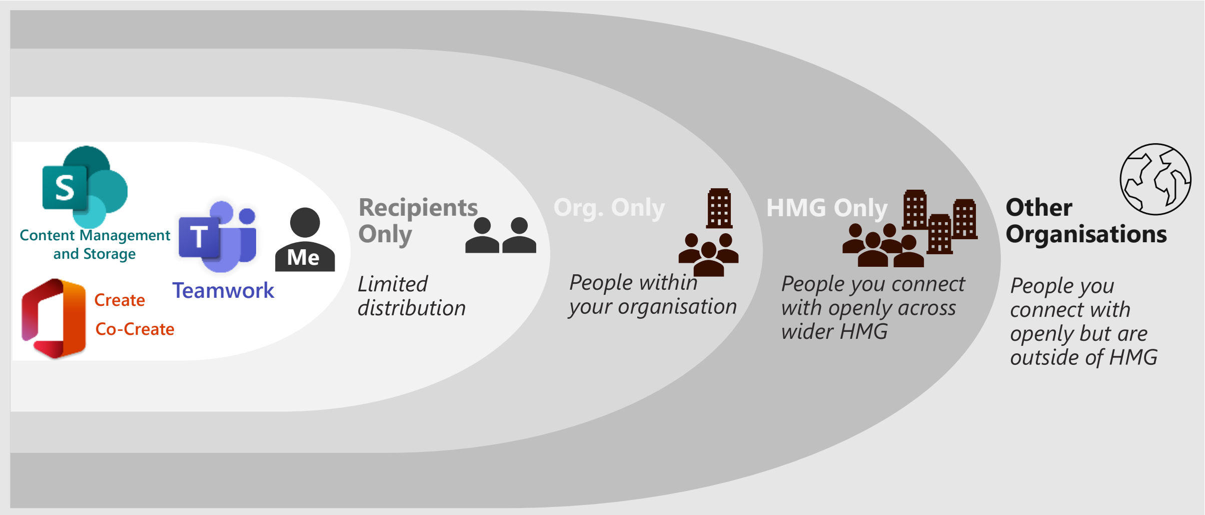
Controls

Content Marking
Encryption

Policy

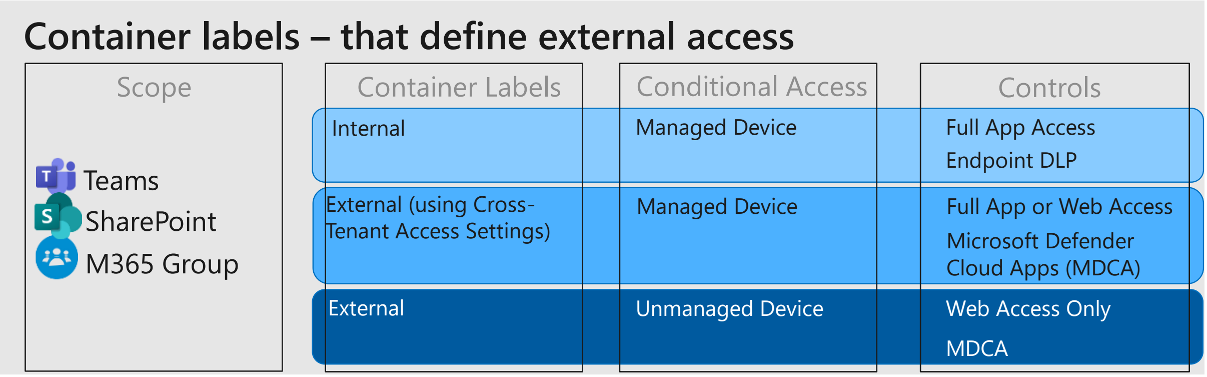
Targeting Users/ Groups
Label Required
Downgrade Justify
Default Label
Auto-Labelling (SITs)

Content labels are used to provide visual indicators for the scope where the document or email should be accessed.


Content Management and Storage
Create
Co-Create
Teamwork
Me
Recipients Only
Limited distribution
Org. Only
People within your organisation
HMG Only
People you connect with openly across wider HMG
Other Organisations
People you connect with openly but are outside of HMG

Container Labels

Container labels that apply to a workload (i.e. SharePoint, Teams or M365 group) where content is stored. The labels are used to define whether External Guest users are allowed to access the container and collaborate with internal member users.



Container labels – that define external access

Scope	Container Labels	Conditional Access	Controls
Teams SharePoint M365 Group	Internal	Managed Device	Full App Access Endpoint DLP
	External (using Cross-Tenant Access Settings)	Managed Device	Full App or Web Access Microsoft Defender Cloud Apps (MDCA)
	External	Unmanaged Device	Web Access Only MDCA

Container labelling applies the sensitivity label at the container. Container labels are named differently from the data labels as they serve a different function – namely to control sharing of the data. These labels provide a visual representation of the Privacy level, Public or Private, and whether external guest users are allowed to be members of the Team or SharePoint site, Internal or External.

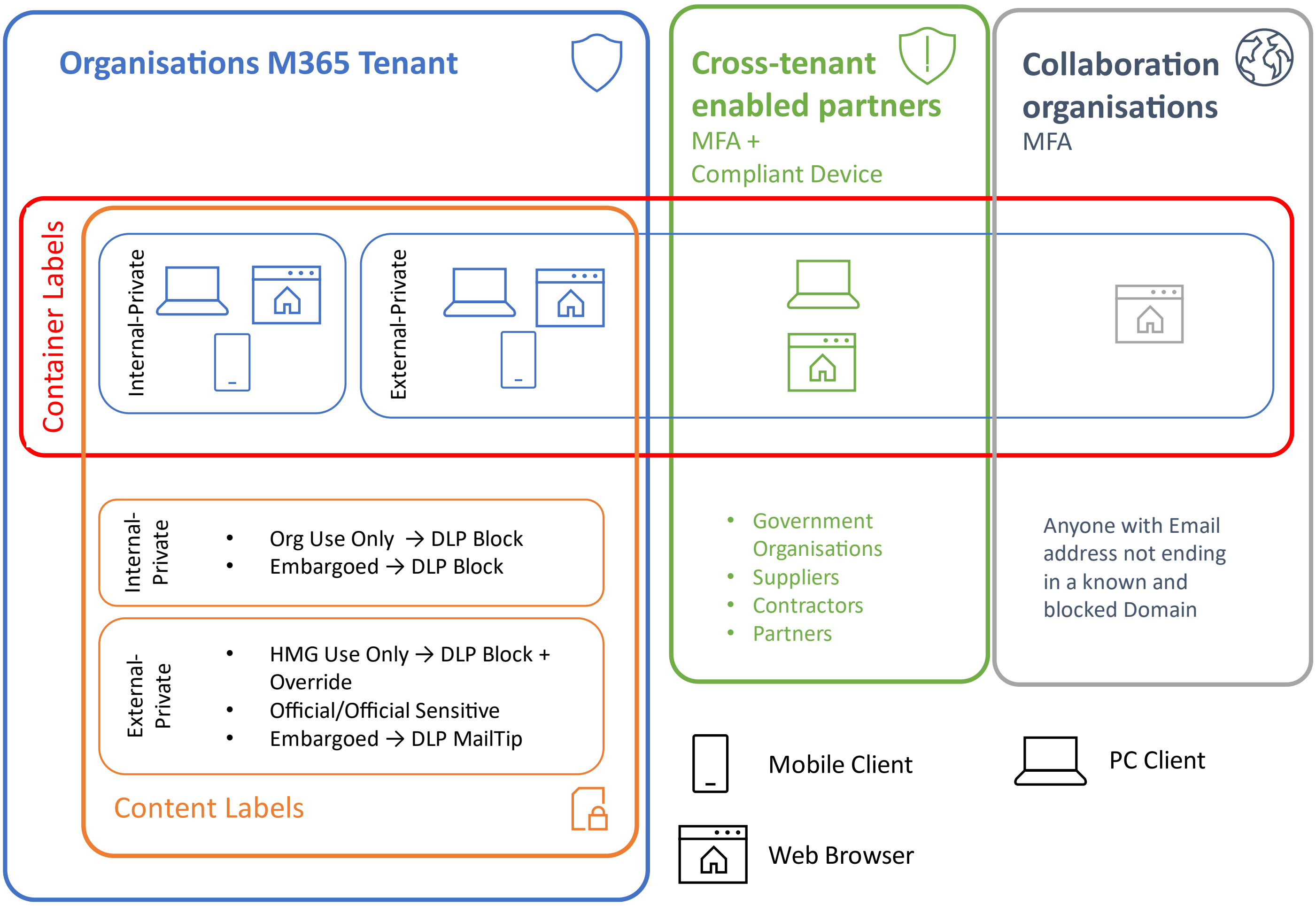

Organisations M365 Tenant
Cross-tenant enabled partners
MFA +
Compliant Device
Collaboration organisations
MFA
Container Labels
Internal-Private
External-Private
Internal-Private
• Org Use Only → DLP Block
• Embargoed → DLP Block
External-Private
• HMG Use Only → DLP Block + Override
• Official/Official Sensitive
• Embargoed → DLP MailTip
Content Labels
• Government Organisations
• Suppliers
• Contractors
• Partners
Anyone with Email address not ending in a known and blocked Domain
Mobile Client
PC Client
Web Browser

Figure 4 describes how sensitivity labels are utilised in two distinct approaches:

1. Content labels that apply to documents or emails and travel with the artifacts
2. Container labels that apply to a workload (i.e. SharePoint, Teams or M365 group) where content can be stored (although this does not mean that data will inherit that label by default, see here for more info).

Content Labels - that follow the data

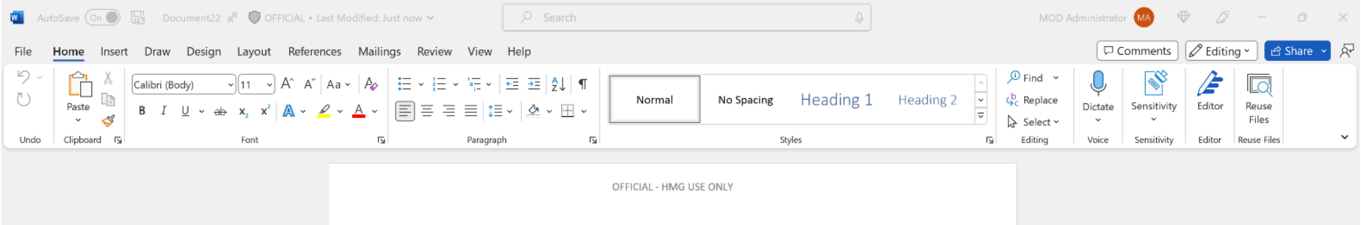
Scope	Data Labels	Controls	Policy
File & Email	Official – Public – HMG Only – Organisation Only – Embargoed Official-Sensitive – HMG Only – Organisation Only – Recipients Only – Embargoed	Content Marking Encryption	Targeting Users/ Groups Label Required Downgrade Justify Default Label Auto-Labelling (SITs)

Container labels – that define external access

Scope	Container Labels	Conditional Access	Controls
Teams SharePoint M365 Group	Internal - Public Internal - Private	Managed Device	Full App Access Endpoint DLP (Enhanced)
	External - Public External - Private	Unmanaged Device	Web Access Only (Enhanced) Full App Access MDCA (Enhanced)

Figure 4: Content and Container label interactions

Whilst visual marking of sensitivity labels provides data handlers with instructions for secure handling, it does not enforce any technical controls to reduce the likelihood of mishandling.



OFFICIAL - HMG USE ONLY

Figure 5: Sensitivity label watermarking – header and footer example

Making use of MPIP achieves a consistent approach to the application of visual markings, helping to standardise their usage and implementation across government.

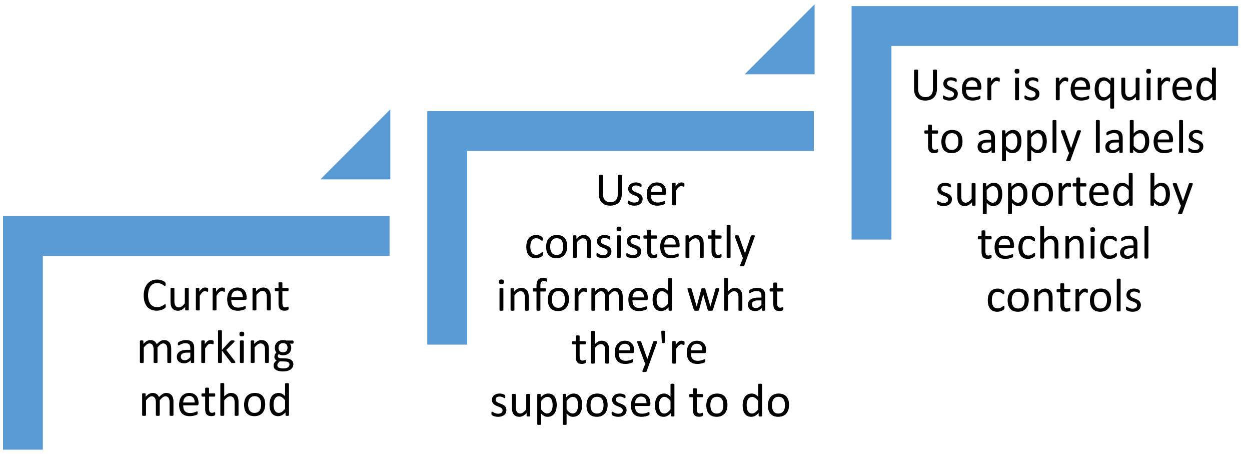

Current marking method
User consistently informed what they're supposed to do
User is required to apply labels supported by technical controls

Figure 6: Outcome based approach

This guidance has been developed to offer a sensible baseline, without mandating that each department follow exactly what is described. Given the variation in operational working practices, it is difficult to be completely prescriptive across all government departments with this guidance. Therefore, it is important that departments fully review what is described in this document, then implement as much as is appropriate to align with your working practices.

The closer you can align to the guidance in this document, the more confidence/control your organisation will have over its data while collaborating both internally and externally. In conjunction with the Cross-Government Guidance previously mentioned, this will lead to increased consistency across the Government community, helping to improve cross-department interoperability.

3 Information Protection principles

This section describes the overarching principles which should be observed regardless of the implementation phase.

Table 2: Information Protection principles explanations.

Principle	Description
Data location	Organisational design principles must state that, where possible, corporate data should reside within your organisational boundary (i.e., Microsoft 365 tenant) as this provides the greatest level of control and monitoring of that data. For more info, refer to: Technical Configuration - Cross-Government Collaboration
Sensitivity label naming	Do not put sensitive info in the label name. Follow the Government Security Classifications Policy (GSCP) naming scheme.
Limit total number of labels	Avoid creating sensitivity labels for every project or department. Additional labels beyond those specified by the GSCP taxonomy should be used with caution.
Latest Microsoft 365 version	Using Microsoft 365's built in labelling requires the latest Office version to obtain all the latest MPIP features. For more info, refer to: Sensitivity label capabilities in Word, Excel, and PowerPoint
Encrypted data co-authoring	After you enable the setting for co-authoring, labelling information for unencrypted files is no longer saved in custom properties. Do not enable this setting if you use any apps, services, scripts, or tools that currently read or write labelling metadata to the old location such as Exchange Message Flow/Transport Rules. For more info, refer to: Metadata changes for sensitivity labels
Labelling priority	Be aware of the labelling priority for labels you configure in the Compliance portal. For more info, refer to: Label priority (order matters)

4 Labelling taxonomy

The updated Government Security Classification Policy (GSCP) looks to help users understand information sensitivities and [any] specific restrictions on information sharing. The guidance covers the following centrally defined label elements of the GSCP at the OFFICIAL tier:

- UK Prefixes,
- Security Classification (at OFFICIAL),
- Additional Marking (i.e. -SENSITIVE)
- Handling Instructions.

OFFICIAL/OFFICIAL-SENSITIVE	<Handling Instruction>	<Descriptor>

PREFIX	CLASSIFICATION	MARKING	HANDLING INSTRUCTION	DESCRIPTOR	CODEWORD	RELEASABILITY
UK	OFFICIAL	-SENSITIVE	HMG USE ONLY	COMMERCIAL	PROJECT ABC	REL EU

This guidance does not automate the application of descriptors, such as those outlined in the GSCP, codewords or releasability marking. If necessary, descriptors can be added as free text outside the visual marking applied by MPIP. For example, including descriptor placeholders in templates for common files like Word and PowerPoint.

A descriptor's purpose is to aid a user by easily identifying certain categories of information with special sensitivities and describe additional access restrictions. Because descriptors are supposed to identify certain categories of information, they are not applicable for the approach to MPIP outlined in this guidance.

MPIP label lists are limited to only one level of nested sub-labels. Adding the descriptor as another level of nested labels is not possible and adding a descriptor to each of the five sub-labels would make the number of options available too complex.

The end-state policies in this guidance enable mandatory labelling where labels are applied to content (files and emails) and workload containers (SharePoint, OneDrive, M365 groups). This requires data originators to apply the appropriate sensitivity label before an email can be sent or before a document can be saved. If the data originator does not apply a label they will be prompted to do so. This ensures that all files and emails are labelled with a GSCP marking.

This guidance does not recommend setting a default label for either email or documents as requiring the user to decide on the appropriate label to apply will reduce information being labelled incorrectly.

> Important
>
> It is acceptable for organisations to make a risk balanced decision to apply a default label to emails only. For example, if you find that your user community are getting 'labelling fatigue' and are inaccurately apply labels as a result. However, if possible, work with your user community to help

> them understand the value in thinking about the sensitivity of the content they are creating and label it appropriately.

The policy also defines that data originators must supply a justification to allow them to downgrade a label to a lower sensitivity label. It stops short of actively preventing label downgrade without administrator approval – but this is a setting that can be enabled if your organisation deems it appropriate. It is recommended to start by allowing users to downgrade labels without administrator approval and monitor use of this feature. Then your policy can be refined accordingly, if the feature is being misused, for example.

> Important
>
> The use of mandatory labelling is the end-state that this guidance recommends. However, as part of the recommended 'Crawl, Walk, Run' phased implementation approach, enforcement of mandatory labelling is not advised until MPIP is more established within the organisation.
>
> Where the encryption is shown as used in the list of protective controls in the following tables, this refers to the end-state for content sensitivity labels. The implementation plan that is outlined in Section 5 does not recommend that encryption is enabled during the pilot / PoC phase (Walk) phase. It should only be enabled when the organisation is comfortable that it will work with internal systems and external partners.

4.1 Content – files & emails

Content labelling applies the label directly to documents and emails. This stamps the data with label metadata which is maintained wherever the data resides. Once a label is applied, the associated controls that the label requires, such as content marking, and encryption are applied. Encryption occurs directly to the file itself, so even if it is shared externally via email, or by using instant messaging or cloud storage services, the encryption remains in place to prevent unauthorised access to the data. With permissions that are linked to the users or groups who are granted access, file content encryption provides granular control over the data, by restricting what actions can be performed with it.

For example, you can define a group of users who can edit and co-author the document and a different group that has viewer only permissions. See here for more info.

The following tables describe the sensitivity labels and the technical controls to be implemented after successful piloting for OFFICIAL-FOR PUBLIC RELEASE, OFFICIAL, OFFICIAL-SENSITIVE, UK OFFICIAL and UK OFFICIAL-SENSITIVE.

> Important
>
> Organisations will need to decide if they need to implement the UK PREFIX within their label lists. Some organisations may not require the UK PREFIX and can therefore keep their label lists simpler.

Table 3: Taxonomy of content for the sensitivity label OFFICIAL-FOR PUBLIC RELEASE

Label	Description	Example	Protective Control
OFFICIAL-FOR PUBLIC RELEASE	OFFICIAL information which can be distributed without restriction because it has been cleared for publication, is already in the public domain or is subject to release in accordance with the Freedom of Information Act 2000. The information is of low sensitivity and there is a need-to-share the information with the general public	policy on gov.uk	Visual marking No encryption No access restrictions

Table 4: Taxonomy of content sensitivity labels for OFFICIAL

Label	Sub-label	Description	Example	Protective Control
OFFICIAL	OFFICIAL (No handling instructions)	Typically information whose compromise would cause limited to no negative consequences for HMG, our partners or to an individual	policy on gov.uk	Visual marking No encryption No access restrictions
	OFFICIAL - EMBARGOED	This marking is applied to information that is only sensitive for a specific period of time and whose sensitivity will be reduced at the end of that period.	Speeches by officials before speech given.	Visual marking Encryption No access restrictions
	OFFICIAL - HMG USE ONLY	Applies to information that should only be shared with other HMG departments, and not with external partners.	Draft policy language	Visual marking Encryption No access restrictions
	OFFICIAL - [INSERT ORG] USE ONLY	Applies to information that should only be shared with the named organisation(s).	Organisation-specific HR policy	Visual marking Encryption Accessible to only users in your organisation
	OFFICIAL - RECIPIENTS ONLY	Indicates that the information must be handled on a strict need-to-know basis by select named individuals. Unauthorised sharing is not justified due to the high risks associated with compromise.	Report of IT Health Check assessment for a system where the report is shared with named individuals only.	Visual marking Encryption No forward, can't remove encryption

Table 5: (not a requirement) Taxonomy of content sensitivity labels for UK OFFICIAL

Label	Sub-label	Description	Example	Protective Control
UK OFFICIAL	OFFICIAL (No handling instructions)	Typically information whose compromise would cause limited to no negative consequences for HMG, our partners or to an individual	policy on gov.uk	Visual marking No encryption No access restrictions
	OFFICIAL - EMBARGOED	This marking is applied to information that is only sensitive for a specific period and whose sensitivity will be reduced at the end of that period. Close as possible to the classification marking.	Speeches by officials before speech given.	Visual marking Encryption No access restrictions

Label	Sub-label	Description	Example	Protective Control
	OFFICIAL - HMG USE ONLY	Applies to information that should only be shared with other HMG departments, and not with external partners.	Draft policy language	Visual marking Encryption No access restrictions
	OFFICIAL - ORGANISATION ONLY	Applies to information that should only be shared with the named organisation(s).	organisation-specific HR policy	Visual marking Encryption Accessible to only users in your organisation
	OFFICIAL - RECIPIENTS ONLY	Indicates that the information must be handled on a strict need-to-know basis by select named individuals. Unauthorised sharing is not justified due to the high risks associated with compromise.	Report of IT Health Check assessment for a system where the report is shared with named individuals only.	Visual marking Encryption No forward, can't remove encryption

Table 6: Taxonomy of content sensitivity labels for OFFICIAL-SENSITIVE.

Label	Sub-label	Description	Example	Protective Control
OFFICIAL-SENSITIVE	OFFICIAL-SENSITIVE (No handling instructions)	Typically information whose compromise would cause limited to no negative consequences for HMG, our partners or to an individual		Visual marking Encryption No access restrictions
	O-S - EMBARGOED	This marking is applied to information that is only sensitive for a specific period and whose sensitivity will be reduced at the end of that period.	Announcement of a new policy or Speech transcript before the speech has been made	Visual marking Encryption No access restrictions
	O-S - HMG ONLY	Applies to information that should only be shared with other HMG departments, and not with external partners.	information relating to crisis response work	Visual marking Encryption No access restrictions
	O-S - ORGANISATION ONLY	Applies to information that should only be shared with the named organisation(s).	security guidance issued by the organisation's security team	Visual marking Encryption No access restrictions
	O-S - RECIPIENTS ONLY	Indicates that the information must be handled on a strict need-to-know basis by select named individuals. Unauthorised sharing is not justified due to the high risks associated with compromise.	Report of IT Health Check assessment for a system where the report is shared with named individuals only.	Visual marking Encryption No forward, can't remove encryption

Table 7: (not a requirement) Taxonomy of content sensitivity labels for UK OFFICIAL SENSITIVE

Label	Sub-label	Description	Example	Protective Control
UK OFFICIAL-SENSITIVE	OFFICIAL-SENSITIVE (No handling instructions)	Typically information whose compromise would cause limited to no negative consequences for HMG, our partners or to an individual		Visual marking Encryption No access restrictions

Label	Sub-label	Description	Example	Protective Control
	O-S - EMBARGOED	This marking is applied to information that is only sensitive for a specific period and whose sensitivity will be reduced at the end of that period.	Announcement of a new policy or Speech transcript before the speech has been made	Visual marking Encryption No access restrictions
	O-S - HMG ONLY	Applies to information that should only be shared with other HMG departments, and not with external partners.	information relating to crisis response work	Visual marking Encryption No access restrictions
	O-S - ORGANISATION ONLY	Applies to information that should only be shared with the named organisation(s).	security guidance issued by the organisation's security team	Visual marking Encryption No access restrictions
	O-S - RECIPIENTS ONLY	Indicates that the information must be handled on a strict need-to-know basis by select named individuals. Unauthorised sharing is not justified due to the high risks associated with compromise.	Report of IT Health Check assessment for a system where the report is shared with named individuals only.	Visual marking Encryption No forward, can't remove encryption

Sensitivity labels applied at the data layer will be read by the Microsoft Purview Data Loss Prevention (DLP) rules, to place further controls on what actions are allowed with that data and support users by providing hints when a user triggers a DLP policy. Refer to Section 5.3.3 Data Loss Prevention (DLP).

4.2 Containers – Microsoft Teams, SharePoint, Microsoft 365 Groups

Containers is the term used to define where content is stored, e.g., Microsoft Teams, SharePoint (including OneDrive for Business) and Microsoft 365 Groups in Microsoft 365.

Container labelling applies the sensitivity label at the container. Container labels are named differently from the data labels as they serve a different function – namely to control sharing of the data. These labels provide a visual representation of the Privacy level, Public or Private, and whether external guest users are allowed to be members of the Team or SharePoint site, Internal or External. Refer to Sensitivity labels for Microsoft Teams for further information.

There is no need to have discrete container label for OFFICIAL-SENSITIVE as the container label refers to the underlying Microsoft 365 workload, the handling instructions of the content is used to enforce the classification, OFFICIAL with additional SENSITIVE marking, and the appropriate handling instruction, e.g., HMG Only.

> Important
>
> With Azure Active Directory (Azure AD B2B), external users collaborate with their identities. Although organizations can issue local usernames and passwords to external users, this approach isn't recommended, refer to Convert local guest accounts to Azure Active Directory B2B guest accounts

Table 8 describes the taxonomy for containers.

Table 8: Taxonomy of container sensitivity labels for OFFICIAL

Container Classification Label	Description	Protective Controls
Internal - Public	A container, Microsoft teams or SharePoint site, containing OFFICIAL data that can be accessed by all internal users in your organisation. A container that should/can be accessed by anyone inside the organisation – staff and colleagues – without additional approval. External guests cannot be added to this container and content cannot be shared with external guests.	Privacy policy: Public – anyone internal can self-service join Everyone can access from approved device/app dependent upon Conditional Access policy evaluation. Internal users can access only from managed devices. External users are not allowed access
Internal - Private	For containers, Microsoft Teams or SharePoint site, containing data that can only be accessed by your staff. A container that should/can only be accessed by named individuals in the organisation. Access is controlled by the owner(s) of the container. External guests cannot be added to this container and content cannot be shared with external guests.	Privacy policy: Private – only owners and members can access. External sharing allowed: No - Site content can be shared with internal users only. Only owners can add members. Internal users can access only from managed devices. External users are not allowed access
External - Public	A container that should/can be accessed by all internal users and Internal guests in your organisation – staff and colleagues – without additional approval. External guests can also access this container. Content inside this container can be shared externally with named individuals.	Privacy policy: Public – any internal user or Internal guests can self-service join External guest can request access. External sharing allowed: Yes - Site content can be shared with new and existing guests. Internal users can access only from managed devices. Everyone can access from approved device/app dependent upon Conditional Access policy evaluation.
External - Private	A container that should/can only be accessed by named individuals in your organisation and external guest users. Access is controlled by the owner(s) of the container. Content can be shared externally with named individuals.	Privacy policy: Private – only owners and members (including invited guests) can access. Only Admins can add External Guests External sharing allowed: Yes - Site content can be shared with new and existing guests. Internal users can access only from managed devices. External users can access from approved device/app dependent upon Conditional Access policy evaluation.[1]

For more information on how sensitivity labels work across Microsoft Teams, SharePoint, and OneDrive, visit the following web pages:

Enable sensitivity labels for Office files in SharePoint and OneDrive

Apply a sensitivity label to content automatically

[1] If Cross-tenant access relationship exists, then desktop or web apps can be used. Refer to Section 5.3.4.1 later in this document.

Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites

The following link describes how to use sensitivity labels to create an isolated team that can be used to provide a collaboration space for sensitive projects with protection that travels with the files that are stored in the team. Refer to Configure a team with security isolation for more details.

Azure AD Conditional Access (CA) is used to enforce access control to containers based upon the label applied. These container sensitivity labels are used to govern which users can access the data and from what device. Conditional access (CA) rules provide an access control mechanism to gate access based on whether the person attempting to view the data is inside the organisation or is an external guest user, and to determine the associated level of trust you can derive for the device they are connecting from.

When combined with CA rules, container sensitivity labels provide context aware access to the container and the data it stores. You define whether the data that resides in that container can:

- Only be accessed by your internal users connecting from a corporate (or managed) device.
- Allow external guests connecting from a guest device (that is not one of your corporate devices joined to your tenant).

For more info, see How to enable sensitivity labels for containers and synchronize labels.

5 Enablement phases – crawl, walk, run

As outlined earlier, we highly recommend a “Crawl-Walk-Run” approach, in which the capabilities are introduced in stages, firstly focusing on elements which cause minimal disruption, such as manual labels without protection, adding basic protection elements in a later stage (e.g. DLP controls to prevent highly confidential items from being accidentally sent outside, or encryption with very broad rights applied), and finally adding more restrictive permissions and tighter controls once you are confident in the use of the technology.

5.1 Pilot Implementation approach

An example approach to implementation of Microsoft Purview Information Protection (MPIP) is provided in Figure 7 below. In this example the Organisation has completed a Crawl phase, preparing the environment ready for the user community to pilot. During the Walk phase a pilot group operates with a set of capabilities applied to them, allowing the organisation to receive feedback which can be used for training, and importantly ensure that business processes are not interrupted by the introduction of features such as file encryption. When the organisation is confident in the results of the pilot, the capabilities will be implemented to the whole organisation, and a new pilot begins. Once all capabilities are implemented an Organisation can consider itself to be in the Run phase and look to apply more advanced capabilities.

> Important
>
> When selecting participants for the pilot groups it is essential to have representatives from all areas of the organisation. The implementation of some Microsoft Purview Information Protection capabilities may have unexpected results with systems such as third-party DLP, Automated data processing, etc.

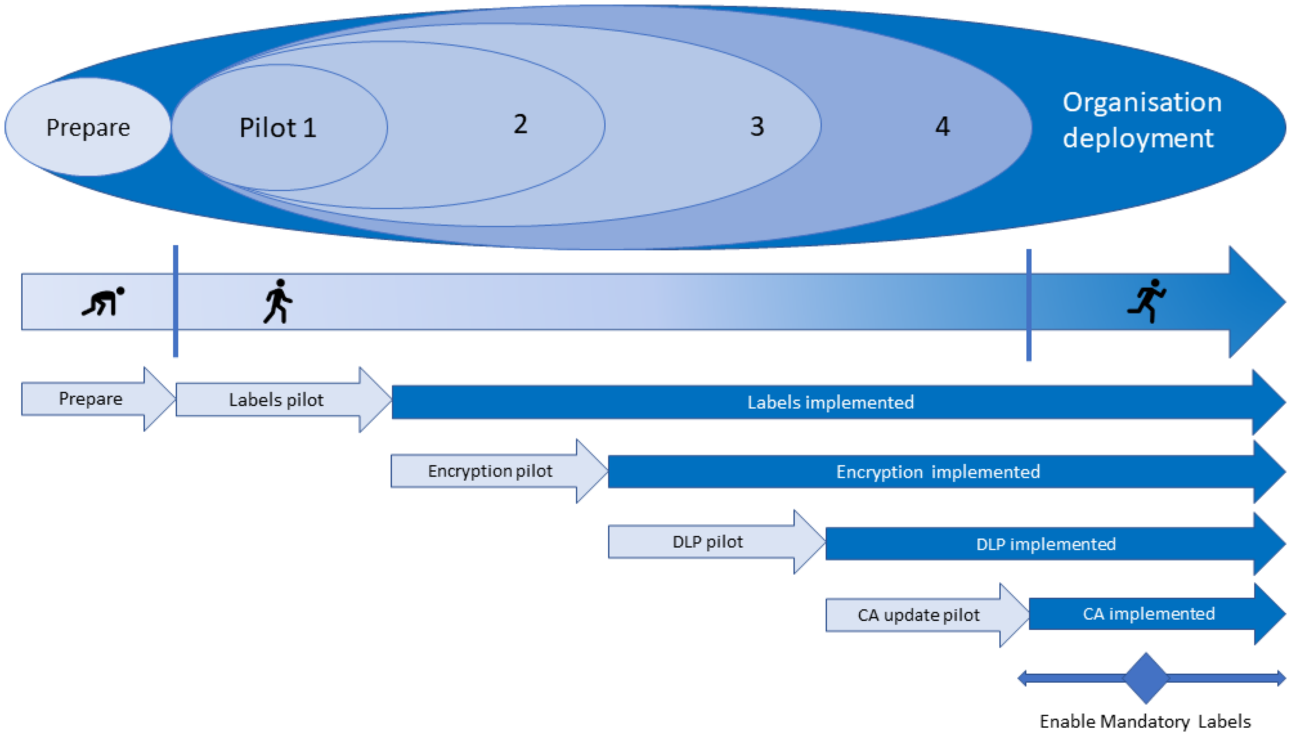


Figure 7 Phased pilot implementation

The process flow illustrated below by Figure 8: Pilot implementation flow is a proposed method for running each of the pilot phases.

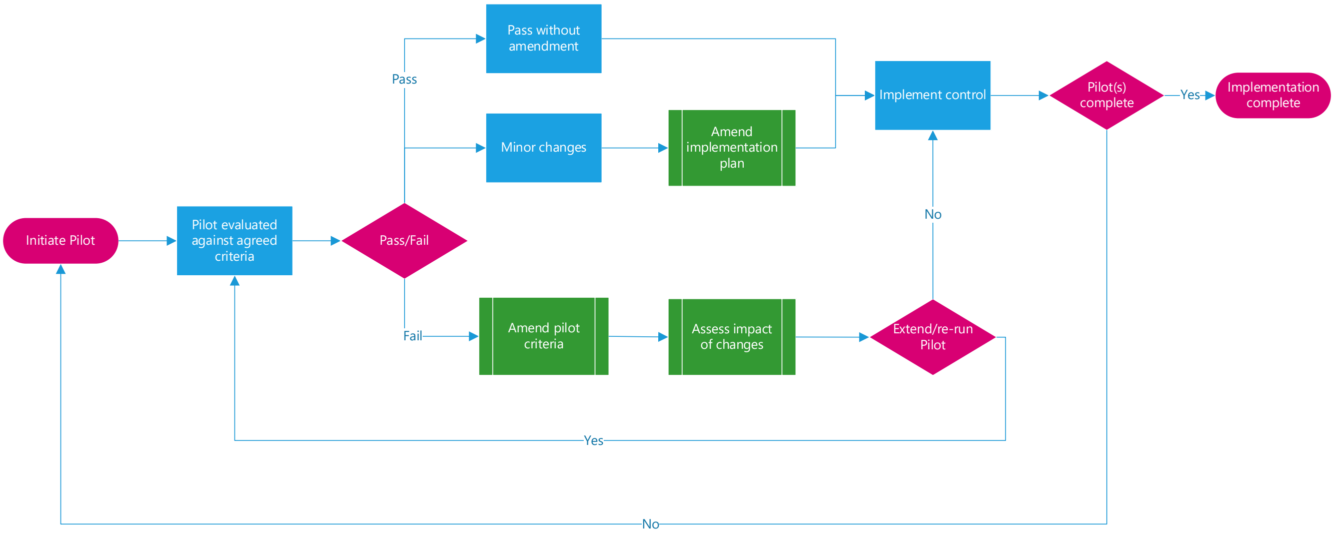


Figure 8: Pilot implementation flow

In Table 9 below a breakdown of the capabilities which could be included for each pilot phase, and the expected acceptance criteria.

Table 9: Pilot phase activities

Capability	Pilot number	Description	Acceptance Criteria
Prepare		Complete activities which prepare for the pilot	Adoption and Change Management (ACM) Approach and Plan.

Capability	Pilot number	Description	Acceptance Criteria
		implementation of Microsoft Purview Information Protection	O365 Groups created. Information Protection Alerts mailbox created. Information Protection Super User accounts created.
Visible labels	1	Deploy sensitivity labels to pilot users to validate that	Are labels visible in Office Apps. Does label apply to email. Does label apply to document. Does label apply to container.
Encryption of content	2	Deploy sensitivity labels to pilot users that include the encryption of content in policy	Encrypted data does not disrupt existing processes (3rd party DLP, CRM automation, etc), or a mitigation is available.
DLP – sensitivity labels	3	Implement Data Loss Prevention rules which use sensitivity labels to detect and inform attempts to share data.	Information marked with the OFFICIAL-DEPT-ONLY' label, is blocked from being shared with people External to the Organisation. User is informed with Tips when attempt is made.
Conditional Access	4	Validate that users, internal and external, can access MPIP protected content and containers based on the sensitivity label applied and the device used.	Access to protected information is blocked when an unauthorised user and/or device is used.
Mandatory labels	Organisational Deployment	Require that sensitivity labels must be applied before email is sent or document is saved	When saving document or sending an email, user is prompted that a

Capability	Pilot number	Description	Acceptance Criteria
			sensitivity label is required if one has not been applied.

5.2 Crawl Phase

The crawl phase describes steps you should perform at the beginning of any deployment, whether your requirements are basic or advanced. It includes steps for education, defining requirements, and evaluation or testing. This phase is primarily to perform planning actions and preparation steps associated with your data classification needs.

The following sections describe the controls that are recommended to be implemented during the Crawl phase for an organisation.

Where possible, organisations should configure as many of the controls as possible to ensure the protection of the information in their Microsoft 365 tenant. Where an organisation chooses not to implement a recommended control they should:

- Determine if the residual risk is organisationally acceptable.
- Can meet organisational compliance obligations.
- Compensating technologies, measures or mitigations should be noted in the organisations' risk register.

The following table lists controls which are expected to be deployed as a baseline level, further details in sections following:

Table 10: Crawl Stage Controls

Control	Action
Cross Gov Guidance	Ensure you have read and configured your tenant according to: Microsoft 365 Guidance for UK Government: Secure Configuration Blueprint Microsoft 365 Guidance for UK Government: External Collaboration
Adoption and Change Management (ACM)	Define your adoption and change management approach.
Pilot users	Work with your organisation to determine an appropriate set of pilot users that span all areas of your environment. Refer to section 5.2.1.1 Identify pilot users
Azure AD M365 groups	Create the required Microsoft 365 groups for targeting purposes. Refer to 5.2.2 Create Azure AD Microsoft 365 groups
Shared Alerting Mailbox	Create an Exchange Online shared mailbox for the purposes of receiving Information Protection and Data Loss Prevention alert messages. Refer to section 5.2.3 Create Information Protection alerts shared mailbox
Super User Privileged Access Group	Create a role-enabled Azure AD group with the Information Protection Super User role, for eligible (and audited) administrative access to encrypted content. Refer to section 5.2.4 Information Protection Super User accounts

Control	Action
Reporting and Monitoring	An important part of a well-managed Information Protection environment is to understand your data and how your user community are handling the sensitivity of it. There are several tools available in the Microsoft Compliance portal to help with data discovery and ongoing monitoring. Refer to section 5.2.4 Information Protection Super User accounts

5.2.1 Adoption and Change Management (ACM)

A key part of your adoption strategy should include support for your end users. Help them to adjust to the real time collaboration approach by encouraging them to embrace the mindset change this requires.

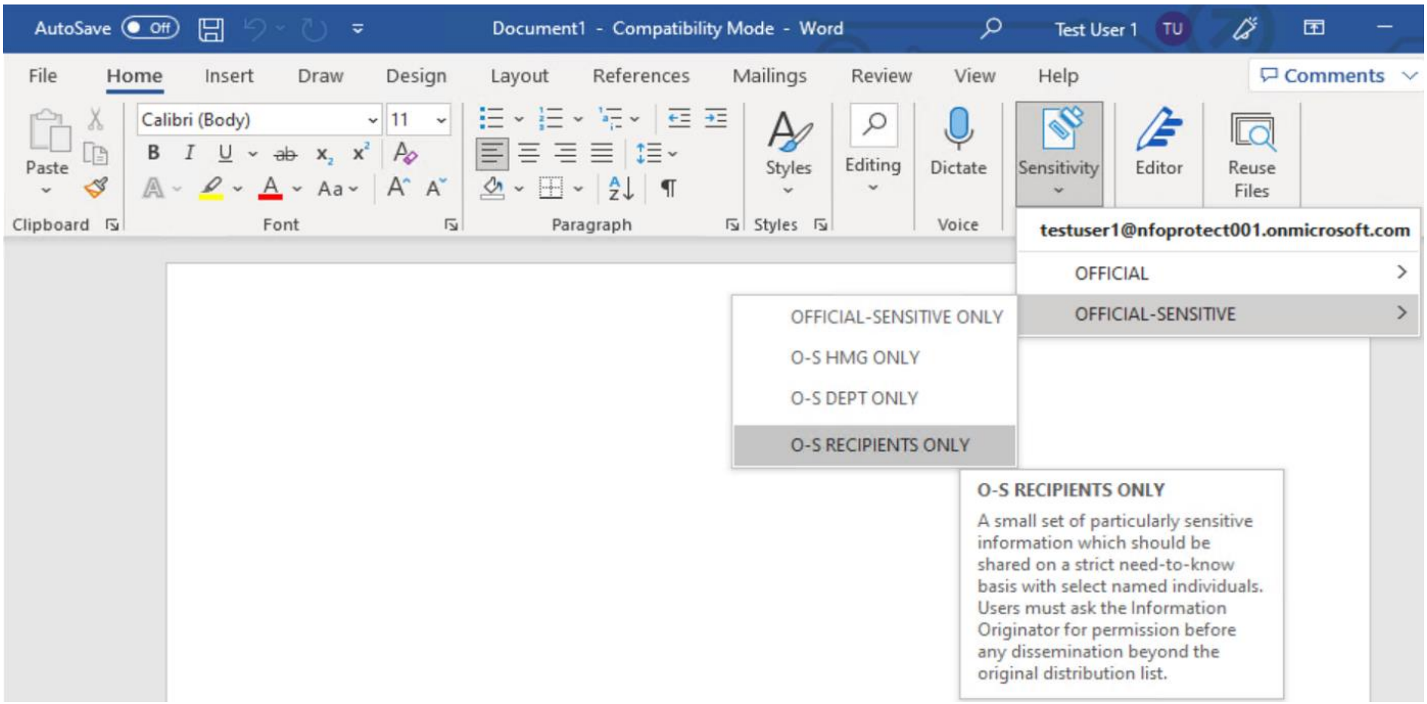
For most organisations, when users are collaborating internally or externally, the use of email is ingrained. Organisations need to support their users and help them rethink how collaboration occurs, both internally and externally, by taking advantage of the capabilities provided by Microsoft 365, secured with Microsoft Purview Information Protection.

> Reminder
>
> The technical deployment of sensitivity labelling is considered the easy part, whereas the user adoption and training are harder to achieve. The better the user education piece, the more successful the overall implementation will be and the more rapidly your organisation can move through the enablement phases.

To help with this, one of the most important parts of the adoption process is to have a clearly defined labelling taxonomy that users can understand and apply.

It is highly recommended to use the taxonomy tables for content, Table 4 and Table 6 in Section 4.1, and container labels, Table 8 in Section 4.2 described earlier. To help support adoption and support users understanding of the taxonomy4.1 it is recommended to publish the taxonomy to your user community. Start by copying and pasting the tables that describe the taxonomy to a new SharePoint page that is accessible by all your users, or an Intranet page. Then customise the table with any additional information that is relevant or specific to your organisations (such as examples of typical data that correspond to the relevant labels) and that will resonate with your users. The point here is to try to help your users make an informed choice about which label they should apply.

Once you have published this taxonomy page, you can make it easy to find by adding the link to the sensitivity label publishing policy



O-S RECIPIENTS ONLY

A small set of particularly sensitive information which should be shared on a strict need-to-know basis with select named individuals. Users must ask the Information Originator for permission before any dissemination beyond the original distribution list.

Figure 9: Sensitivity label tooltip

This can also take the form of a label tooltip (see Figure 9 above for an example) for quick reference or for more detail the Tooltip can also include the link to a web-page or SharePoint site can also help, as described above..

For more info, visit the following page: Provide a link to a custom help page

- **Support users using correct labels before deploying.** Conduct a practical validation to see how accurate your users are at using these labels. One option is to create a digital training package, such as one where users receive an email with a range of mock sensitive documents attached. Send it to a subset of users asking them to open each document in turn and label it. They don't even need to report the results, since you will be able to see how they labelled each document in the Activity Explorer in the Compliance Centre portal. You can alternatively do an offline activity, by setting baskets in the office's entrance, printing copies of a mix of pretend sensitive documents, and putting them in a pile at the entrance with a sign that says "take one and put it in the corresponding basket". Users usually do this exercise consciously and it allows you to get a very representative idea of how well your users understand policies and labelling taxonomy. After you have done an exercise, you can validate the accuracy of user's actions and tune your labels and training materials accordingly.
- **Socialise labels so they become part of the organization's natural language**. While experience indicates the sensitivity label UI is simple enough that most users don't need to be trained in its use, it is important to perform an awareness campaign in which the meaning of the different labels and the importance of their use is highlighted (i.e. awareness emails, physical posters, etc.). The objective of such a campaign is that users incorporate the organization's labels as part of their natural language and that can intuitively assign the appropriate label to their documents/content.

The following table lists some of the recommended adoption and change management activities that should be completed during this phase:

Table 11: ACM checklist

ACM item	Completed
Define your ACM approach	

ACM item	Completed
Ensure tenant is configured according to the cross-government collaboration guidance	
Publish a label taxonomy page (SharePoint is a good place for this) that explains the labels and gives organisational specific usage examples – this link can be published with the label policy to help users understand which label to use	
Determine what data you have and which of the container labels match that data	
Collate a list of the external organisations (and their associated domain names) that you currently communicate with	
Define the label override/exception process – describe what the 'no protections' is intended for and educate your user community on its use (then add to the taxonomy page)	
Perform a discovery exercise to understand whether your organisation uses any content inspection (for things like email or custom developed applications) that may break when encryption is introduced	

5.2.1.1 Identify pilot users

It is recommended to identify the relevant pilot users from across your organisation to help with the introduction and testing of the MPIP solutions. Try to identify a cross-section of users that span the entire organisation, by ensuring you have representation from all departments.

Once you have established your pilot user working group, meet with them to understand their work patterns with regards to the Microsoft 365 data they generate and consume. Where do they store their data? What Office applications do they use most regularly? How do they share data? Who do they typically collaborate with? These are just a few of the sorts of questions you should seek answers to, which will help in your planning for the adoption of the Microsoft Purview Information Protection suite of tools into your environment.

Once the pilot user groups have been established, these will be used in your labels pilot phase (see Section 5.3.1 Labels).

5.2.2 Create Azure AD Microsoft 365 groups

To prepare for the deployment of Microsoft Purview Information Protection, creation of Azure AD Microsoft 365 groups is required.

AzureAD Microsoft 365 Dynamic User group example:

- The following dynamic user rule will include only tenant full members and no guests (DEPT ONLY):

(user.userType -eq "Member") and (user.userPrincipalName -notContains "#EXT#@")

To include only guest users with a gov.uk address, create an AAD group using this dynamic user query (HMG ONLY):
(user.userType -eq "Guest") and (user.userPrincipalName -Contains "_gov.uk#EXT#@")

The groups below (in Table 12) show some dynamic membership rules that serve as examples. You will need to review these and adjust to suit your environment. The following groups are recommended to align with the sensitivity label publishing policies during the pilot phase and then later phases once you enable encryption.

> ### Important
>
> The groups described below describe the end-state once the pilots have been completed and mandatory labelling enabled. All groups should be created as 'Microsoft 365 groups – with no associated Team'.
>
> The Dynamic group rules should be tested for accuracy and validity during the pilot, e.g., the "HMG-ONLY" dynamic group will only pick up *.gov.uk Guest users so this should be tested.
>
> An alternate way to achieve this outcome is to add the domains directly to the Protection policy, this does require more effort to maintain but will ensure that there is no delay for external guest users to be picked up by the Dynamic rule processing.

Table 12: Azure AD Microsoft 365 groups

Group name	Description	M365 group dynamic user rule
UK GOV Classification Pilot	Pilot Targeting group for sensitivity label policy publishing	Assigned User group
UK GOV Classification	Targeting group for sensitivity label policy publishing at the wider user population in your organisation.	Assigned User group
ORG-ONLY	Dynamic user group containing only staff from your organisation	**(user.userType -eq "Member") and (user.userPrincipalName -notContains "#EXT#@")**
HMG-ONLY	Dynamic user group containing HMG guests	**(user.userType -eq "Guest") and (user.userPrincipalName -Contains "_gov.uk#EXT#@")**
OFFICIAL-*ORG*-ONLY-CO-AUTHOR	Co-Author rights for encryption on OFFICIAL-*ORG*-ONLY	**(user.userType -eq "Member") and (user.userPrincipalName -notContains "#EXT#@")**
OFFICIAL-EMBARGOED-CO-OWNER	Co-Author rights for encryption on OFFICIAL EMBARGOED	–
OFFICIAL-EMBARGOED-VIEWER	Viewer rights for encryption on OFFICIAL EMBARGOED	–
OFFICIAL-HMG-ONLY-CO-AUTHOR	Co-Author rights for encryption on OFFICIAL HMG ONLY	**(user.userType -eq "Guest") and (user.userPrincipalName -Contains "_gov.uk#EXT#@")**
OFFICIAL-SENSITIVE-*ORG*-ONLY-CO-AUTHOR	Co-Author rights for encryption on OFFICIAL-SENSITIVE-*ORG*-ONLY	**(user.userType -eq "Member") and (user.userPrincipalName -notContains "#EXT#@")**

Group name	Description	M365 group dynamic user rule
OFFICIAL-SENSITIVE-HMG-ONLY-CO-AUTHOR	Co-Author rights for encryption on OFFICIAL-SENSITIVE HMG ONLY	**(user.userType -eq "Guest") and (user.userPrincipalName -Contains "_gov.uk#EXT#@")**

Table 13: Azure AD Microsoft 365 groups

5.2.3 Create Information Protection alerts shared mailbox

It is recommended to create a dedicated mailbox that can be shared amongst the appropriate administrators, to receive MPIP alerts – if one does not already exist.

For more info, visit the following page: Shared mailboxes in Exchange Online

5.2.4 Information Protection Super User accounts

Super user accounts have the necessary rights to gain administrative access to any data that is protected by Information Protection. If a user protects a piece of data without granting any other users access, and then leaves the organisation – a user who has super user rights can access that protected content and make changes to enable other users to gain access.

The super user role can be assigned to a role-enabled Azure AD group, which can be converted to a privileged access group (PAG). To gain the super user rights, users then need to be made eligible via privileged identity management (PIM). This provides a just-in time (JIT) model for elevating into the super user role, that is audited and time-limited – avoiding users being permanently assigned (i.e., preventing 'standing access') to this role.

Refer to appendix for detailed configuration instructions.

5.2.5 Create feedback loop mechanism

At this phase, setup a method for your users to begin capturing feedback. This will be required to collect reports of issues and provide a way to track them to resolution. It will also be used to enable users to start recording keywords that will feed into Sensitive Information Types (SITs). This may be a mailbox, SharePoint site or Teams channel.

5.2.6 Introduction to Sensitive Information Types (SITs)

Sensitive Information Types (SITs) provide a level of system automation to recommend (or even auto-apply) specific labels when certain keywords are detected. SITs are dictionaries of words and definitions of how many times they must occur for them to be considered 'interesting' data for the purposes of system detection.

As you begin working with your pilot users, you should make them aware of what SITs are and their value. For SITs to be of real value to your organisation, it requires input from your users to provide the relevant keywords that the detection system will scan for.

During your pilot phases, users can record examples of these regularly used keywords and the indication of their sensitivity within your organisation. They might be project specific words or phrases, department names or anything that can be used to identify data that is of a sensitive nature. Getting your users to think about these keywords will begin to shape the resulting sensitive information types (SITs). These serve as the foundation for the technical controls implemented in the Data Loss Prevention (DLP) policies described in the run phase later of this guidance.

> Note: implementation of SITs have been intentionally placed in the run phase of this guidance. This is because experience shows that SITs can complicate and ultimately delay your Microsoft Purview Information Protection rollout if you begin attempting to integrate them too early in your environment.

For further information on SITs refer to: Learn about sensitive information types - Microsoft Purview (compliance) | Microsoft Learn

5.2.6.1 Built-in Sensitive Information Types

The Microsoft Compliance admin centre comes pre-loaded with over 100 SITs, most of them related to identifying and locating personal data, financial data, and health-related data specific to various regulations that organizations may be subject to around the world. These built-in sensitive information types can help identify and protect credit card numbers, bank account numbers, passport numbers, and more, based on patterns that are defined by a regular expression (regex) or a function. To learn more, see What the sensitive information types look for.

In addition to the built-in SITs, you can also create custom info types via three methods, including PowerShell, custom rules via exact data match (EDM), and through the Compliance Center admin UI. You can also customise an existing, built-in SIT to make it more relevant and accurate for your environment.

Custom Sensitive Information Types

If an organization needs to identify and protect a specific type of sensitive information not covered by built-in SITS, they can create a custom sensitive information type or modify an existing, built-in type.

A custom SIT defines org-specific 'interesting data' that the system uses to know what to look for. Once you define these keywords their relevance and importance, automated processing examines your data and identifies instances that match the criteria you specify. This then alerts you to the presence of such data and enables action to be taken, ultimately allowing you to apply the appropriate protections.

Refer to the following articles which explore these in more depth:

- Customize a built-in sensitive information type
- Custom sensitive information types
- Create a custom sensitive information type in the Security & Compliance Center
- Create a custom sensitive information type in Security & Compliance Center PowerShell
- Create custom sensitive information types with Exact Data Match based classification

For more info visit the following page: Learn about sensitive information types

Exact Data Match

Exact Data Match (EDM) is a custom sensitive information type (SIT) that uses exact or nearly exact data values, instead of one that finds matches based on generic patterns. Using EDM, you can create a custom sensitive information type that is designed to:

- be dynamic and easily refreshed.
- be more scalable.
- result in fewer false-positives.
- work with structured sensitive data.
- handle sensitive information more securely, not sharing it with anyone, including Microsoft.
- be used with several Microsoft cloud services.

EDM finds matches by comparing content against a table of sensitive data that you define. The match testing is done using a combination of traditional rules along with patterns, to ensure that the matched data is an actual instance of data you want to find and protect. At its core, EDM works by comparing strings in your documents and emails against values in a table of sensitive data you provide, to find out if the values in your content are present in the table by comparing one-way cryptographic hashes.

For more info, visit the following page: Learn about exact data match based sensitive information types

Trainable Classifiers

This classification method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of classification is more about using a classifier to 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.

There are two types of classifiers: pre-trained and custom. Pre-trained are made available and ready to use in Microsoft 365. Custom classifiers are ones you must create yourself.

To create a custom trainable classifier, feed it (between 50 to 500) data examples that should be considered positive matches. Once it processes those examples, 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.

When you publish the classifier, it sorts through items in locations like SharePoint Online, Exchange, and OneDrive, and classifies the content. After you publish the classifier, you can continue to train it using a feedback process that is like the initial training process.

For more info, visit the following page: Get started with trainable classifiers

5.2.7 Reporting and Monitoring

An important step on the Information Protection journey involves knowing your data. Understanding what sensitive data your organisation has and where it is stored, are a vital part of a well-defined information governance strategy. Microsoft Purview Information Protection provides several tools (as described below) to help you discover and manage your sensitive data.

It is important to understand what labels your users are applying, to ensure accuracy and avoid misuse (either accidental or deliberate).

Use Activity Explorer during your pilot phases (and beyond) to monitor how your users are using labels in your organisations.

5.2.7.1 Activity Explorer

Activity Explorer allows you to monitor what's being done with your labelled content. Activity Explorer provides a historical view of activities on your labelled content. The activity information is collected from the Microsoft 365 unified audit logs, transformed, and made available in the Activity Explorer UI. Activity Explorer reports on up to 30 days’ worth of data.

For more info, visit the following page: Get started with activity explorer

5.2.7.2 Content 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 organization. This may involve establishing a process and assigned responsibility to regularly investigate the presence and location of sensitive information.

This provides a starting point for identifying overall sensitive information risk exposure and protection needs throughout Microsoft 365.

For more info, visit the following page: Getting started with Content Explorer

5.2.7.3 Content Search

In addition to the Content Explorer, organizations have access to the "Content Search" capability to produce custom searches for and find personal data in their environment, using advanced search criteria and custom filters.

Additional insights on investigative and remediation techniques for personal data in Microsoft 365 are provided in the article: Monitor and respond to data privacy incidents.

5.2.7.4 Compliance Manager

Microsoft Compliance Manager provides a dashboard that helps you manage your organization's compliance requirements. Use it to view a score of your environment against recommended practices for a pre-defined compliance standard (such as GDPR).

To learn more about Microsoft Compliance Manager (MSCM) visit the following webpage: Microsoft Compliance Manager (MSCM) Ninja Training

5.3 Walk Phase

The second stage builds the foundation for a successful, scalable, and sustainable deployment. In this phase you deploy the pilot phases by deploying into a development tenant or directly into production.

The following controls are included in the Walk phase:

Table 14: Walk controls

Control	Action
Create sensitivity labels	Use the Microsoft 365 compliance center to create and configure sensitivity labels. Refer to Section 5.3.1 Labels pilot
Publish sensitivity labels	Use the Microsoft 365 compliance center to configure and publish sensitivity labels. Refer to section 5.3.1.2 Publish sensitivity labels
Enable Content encryption	Use the Microsoft 365 compliance center to create and configure Encryption for Sensitivity Labels Refer to Section 5.3.2 Encryption pilot
Configure Data Loss Prevention (DLP) for emails & files	Use the Microsoft 365 compliance center to create and configure DLP policies. Refer to section 5.3.3 Data Loss Prevention (DLP)

Control	Action
Validate updates to Conditional Access policies	Refer to Section 5.3.4 Conditional Access pilot

5.3.1 Labels pilot

The labels pilot is the first of the pilots used to implement MPIP into your organisation. The aim of this pilot is to create and deploy sensitivity labels to pilot users to allow them to validate that the correct visible indicator is applied to emails and documents when selected.

During the Labels pilot no encryption is applied to content and the labelling is optional. This is to allow your users to become familiar with the labelling taxonomy and applying labels to documents.

Use Activity Explorer to track adoption of label use on content in your organisation. This is a key indicator of how successful your communications plan has been and how users are finding the change to content creation and sharing. The information presented in Activity Explorer will be an important consideration when determining when to move to mandatory labelling as the end-state for MPIP.

The appropriate list of pilot users should already have been identified by completing the recommendations made earlier in this document, during the Crawl Phase (see Section 5.2.1.1 Identify pilot users).

It is unlikely that the standard labels will have an impact on the normal operation of the system. However, if you ensure that your pilot group consists of individuals from all areas of the organisation, any issues that arise can be identified and resolved. This becomes more important once you progress to the sensitivity labels that apply encryption to content. So, it is beneficial to get this right before moving on to that stage. Refer to the encryption pilot section for further guidance.

After successful completion of your sensitivity label pilot, you will need to create a duplicated set of the labels to publish to your entire organisation. This duplicated set will represent the final set of labels that will be consumed by your organisation, once all label pilots (including the later encryption label pilot) have been successfully completed.

5.3.1.1 Create sensitivity labels

Sensitivity labels are the 'tagging' mechanism by which the Information Protection policy engine determines what technical controls to enforce. These labels are also used in context aware access controls, such as in Conditional Access and DLP policies.

To create a new sensitivity label, browse to the Microsoft 365 compliance center portal. Navigate to Information protection | Labels and click the 'Create a label' button.

Follow the wizard to create a new sensitivity label.

You will need to provide the following data:

- Label name and description (note: the description corresponds to the tool-tip message text the users will see when they hover over the label in the Microsoft 365 application).
- Scope for the label targeting:
  - Files & emails – apply labels to emails and Office files
  - Groups & sites – apply labels to Teams, Microsoft 365 Groups and SharePoint sites (i.e. 'container' labels)
- Decide whether to apply encryption and visual markings
- For container labels, configure associated protections to control internal/external user access and sharing

For more info, visit the following page: Create and configure sensitivity labels

If you were already using the now deprecated Azure Information Protection (AIP) labelling, you should refer to the following link for migration steps to the new Unified Labelling solution: Tutorial - Migrating from the Azure Information Protection (AIP) classic client to the unified labelling solution | Microsoft Docs

The basic flow for deploying and applying sensitivity labels is as follows:

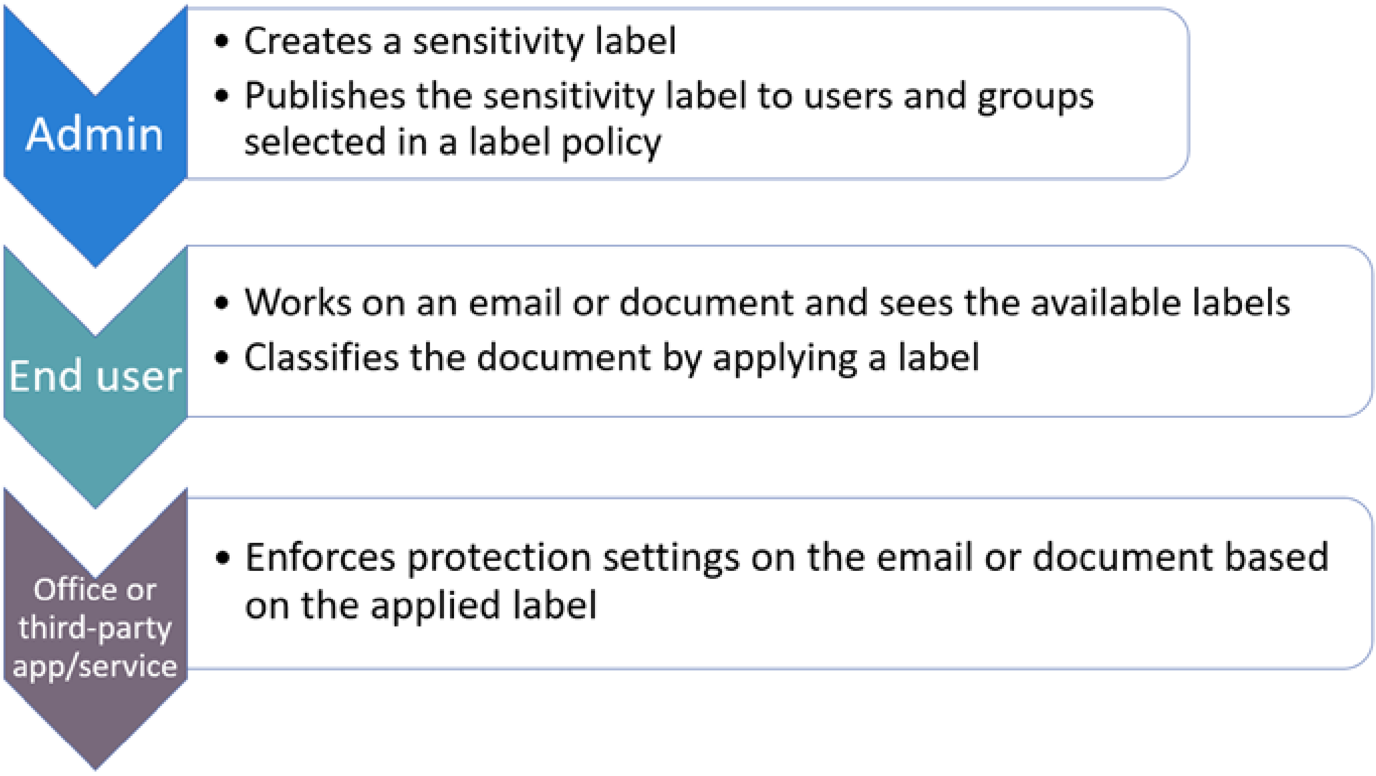

Admin
• Creates a sensitivity label
• Publishes the sensitivity label to users and groups selected in a label policy
End user
• Works on an email or document and sees the available labels
• Classifies the document by applying a label
Office or third-party app/service
• Enforces protection settings on the email or document based on the applied label

Figure 10: Label implementation

When you have published sensitivity labels from the Microsoft 365 compliance centre, they start to appear in Office apps for users to classify and protect data as it's created or edited.

The following tables, detail the recommended content sensitivity labels for UK public sector organisations.

OFFICIAL-FOR PUBLIC RELEASE Content label

In the Microsoft Purview Information Protection portal, create the label.

Table 15 OFFICIAL-FOR PUBLIC RELEASE Applied sensitivity label for content

Create a label step		Action
Name & description	Name:	OFFICIAL-FOR PUBLIC RELEASE
	Display name:	OFFICIAL-FOR PUBLIC RELEASE
	Description for users:	OFFICIAL information which can be distributed without restriction because it has been cleared for publication, is already in the public domain or is subject to release in accordance with the Freedom of Information Act 2000.

Create a label step		Action
		The information is of low sensitivity and there is a need-to-share the information with the general public
	Description for admins:	OFFICIAL-FOR PUBLIC RELEASE label
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Unticked
	Mark the content of files:	Ticked
Content marking	Add a header | Text:	OFFICIAL-FOR PUBLIC RELEASE
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL-FOR PUBLIC RELEASE
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

OFFICIAL Content labels

In the Microsoft Purview Information Protection portal, create the initial label as the parent label by clicking the '+ Create a label' link:

Table 16 OFFICIAL sensitivity parent label for content

Create a label step		Action
Name & description	Name:	OFFICIAL
	Display name:	OFFICIAL
	Description for users:	Typically, information whose compromise would cause limited to no negative consequences for HMG, our partners or to an individual.
	Description for admins:	OFFICIAL parent label

Create a label step		Action
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Unticked
	Mark the content of files:	Ticked
Content marking	Add a header | Text:	OFFICIAL
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Create the remainder of these labels as **sub-labels of the OFFICIAL parent label** by clicking the three ellipsis and selecting the '+ Add sub label' option:

Table 17 OFFICIAL | OFFICIAL sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL – no handling instructions
	Display name:	OFFICIAL
	Description for users:	Typically, information whose compromise would cause limited to no negative consequences for HMG, our partners or to an individual.
	Description for admins:	OFFICIAL sub-label of OFFICIAL with no marking or handling instructions
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Unticked

Create a label step		Action
	Mark the content of files:	Ticked
Content marking	Add a header | Text:	OFFICIAL
	Add a header | Font size:	Use your organisation’s default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL
	Add a footer | Font size:	Use your organisation’s default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 18 OFFICIAL | EMBARGOED sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL - EMBARGOED
	Display name:	EMBARGOED
	Description for users:	This marking is applied to information that is only sensitive for a specific period and whose sensitivity will be reduced at the end of that period.
	Description for admins:	EMBARGOED for OFFICIAL
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always

Create a label step		Action
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	Users in my organisation	Co-Owner
	Any authenticated user	Co-Author
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	OFFICIAL - EMBARGOED
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL - EMBARGOED
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 19 OFFICIAL | HMG USE ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL - HMG USE ONLY
	Display name:	HMG USE ONLY
	Description for users:	Applies to information that should only be shared with other HMG departments, and not with external partners.
	Description for admins:	HMG-ONLY for OFFICIAL
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked

Create a label step		Action
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-HMG-ONLY-CO-AUTHOR@*tenantnamehere*	Co-Author
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	OFFICIAL - HMG USE ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL - HMG USE ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 20 OFFICIAL | ORG USE ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL - *[INSERT ORG]* USE ONLY
	Display name:	*[INSERT ORG]* USE ONLY
	Description for users:	Applies to information that should only be shared with the named organisation(s).
	Description for admins:	*[INSERT ORG]* USE ONLY for OFFICIAL
Scope	Files & emails:	Ticked

Create a label step		Action
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-*ORG*-ONLY-CO-AUTHOR@*tenantnamehere*	Co-Author
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	OFFICIAL - *[INSERT ORG]* USE ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL - *[INSERT ORG]* USE ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 21 OFFICIAL | RECIPEINTS ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL - RECIPIENTS ONLY
	Display name:	RECIPIENTS ONLY

Create a label step		Action
	Description for users:	Indicates that the information must be handled on a strict need-to-know basis by select named individuals. Unauthorised sharing is not justified due to the high risks associated with compromise.
	Description for admins:	RECIPIENTS ONLY for OFFICIAL
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails[2]:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Let users assign permissions when they apply the label
	In Outlook, enforce one of the following restrictions:	Do Not Forward
	In Word, PowerPoint and Excel, prompt users to specify permissions:	Ticked
Content marking	Add a header | Text:	OFFICIAL - RECIPIENTS ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL - RECIPIENTS ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

[2] Refer to Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs for more details

Table 22 UK OFFICIAL sensitivity parent label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL
	Display name:	UK OFFICIAL
	Description for users:	Typically, information whose compromise would cause limited to no negative consequences for HMG, our partners or to an individual.
	Description for admins:	UK OFFICIAL parent label
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Unticked
	Mark the content of files:	Ticked
Content marking	Add a header | Text:	UK OFFICIAL
	Add a header | Font size:	Use your organisation’s default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL
	Add a footer | Font size:	Use your organisation’s default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Create the remainder of these labels as sub-labels of the UK OFFICIAL parent label by clicking the three ellipsis and selecting the ‘+ Add sub label’ option:

Table 23 UK OFFICIAL | OFFICIAL - No-Restrictions-Applied sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL – no handling instructions
	Display name:	OFFICIAL
	Description for users:	Typically, information whose compromise would cause limited to no

Create a label step		Action
		negative consequences for HMG, our partners or to an individual.
	Description for admins:	UK OFFICIAL with no marking or handling instructions
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Unticked
	Mark the content of files:	Ticked
Content marking	Add a header | Text:	UK OFFICIAL
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 24 UK OFFICIAL | EMBARGOED sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL - EMBARGOED
	Display name:	EMBARGOED
	Description for users:	This marking is applied to information that is only sensitive for a specific period and whose sensitivity will be reduced at the end of that period.
	Description for admins:	EMBARGOED for UK OFFICIAL
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked

Create a label step		Action
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-EMBARGOED-CO-OWNER@*tenantnamehere*	Co-Owner
	OFFICIAL-EMBARGOED-REVIEWER@*tenantnamehere*	Reviewer
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	UK OFFICIAL - EMBARGOED
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL - EMBARGOED
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 25 UK OFFICIAL | HMG USE ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL - HMG USE ONLY
	Display name:	HMG USE ONLY

Create a label step		Action
	Description for users:	Applies to information that should only be shared with other HMG departments, and not with external partners.
	Description for admins:	HMG-ONLY for UK OFFICIAL
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-HMG-ONLY-CO-AUTHOR@*tenantnamehere*	Co-Author
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	UK OFFICIAL - HMG USE ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL - HMG USE ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table UK OFFICIAL | ORG USE ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL - *[INSERT ORG] USE ONLY*
	Display name:	[INSERT ORG] USE ONLY
	Description for users:	Applies to information that should only be shared with the named organisation(s).
	Description for admins:	*ORG*-ONLY for UK OFFICIAL
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-*ORG*-ONLY-CO-AUTHOR@*tenantnamehere*	Co-Author
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	UK OFFICIAL - *[YOUR ORG]* USE ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL - *[YOUR ORG]* USE ONLY
	Add a footer | Font size:	Use your organisation's default

Create a label step		Action
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 26 UK OFFICIAL | RECIPEINTS ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL - RECIPIENTS ONLY
	Display name:	RECIPIENTS ONLY
	Description for users:	Indicates that the information must be handled on a strict need-to-know basis by select named individuals. Unauthorised sharing is not justified due to the high risks associated with compromise.
	Description for admins:	RECIPIENTS ONLY for UK OFFICIAL
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails[3]:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Let users assign permissions when they apply the label
	In Outlook, enforce one of the following restrictions:	Do Not Forward
	In Word, PowerPoint and Excel, prompt users to specify permissions:	Ticked
Content marking	Add a header | Text:	UK OFFICIAL - RECIPIENTS ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black

[3] Refer to Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs for more details

Create a label step		Action
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL - RECIPIENTS ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

OFFICIAL-SENSITIVE Content labels

In the Microsoft Purview Information Protection portal, create the initial label as the parent label by clicking the '+ Create a label' link:

Table 27 OFFICIAL-SENSITIVE sensitivity parent label for content

Create a label step		Action
Name & description	Name:	OFFICIAL-SENSITIVE
	Display name:	OFFICIAL-SENSITIVE
	Description for users:	Applies to OFFICIAL information that is not intended for public release and could be of some interest to threat actors. A compromise is likely to cause moderate damage to the work or reputation of the organisation and/or HMG.
	Description for admins:	OFFICIAL-SENSITIVE parent label
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Unticked
	Mark the content of files:	Ticked
Content marking	Add a header | Text:	OFFICIAL-SENSITIVE
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center

Create a label step		Action
	Add a footer | Text:	OFFICIAL-SENSITIVE
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Create the remainder of these labels as sub-labels of the OFFICIAL-SENSITIVE parent label by clicking the three ellipsis and selecting the '+ Add sub label' option:

Table 28 OFFICIAL-SENSITIVE | O-S OFFICAL sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL-SENSITIVE – no handling instructions
	Display name:	OFFICIAL-SENSITIVE
	Description for users:	Typically, information whose compromise would cause limited to no negative consequences for HMG, our partners or to an individual.
	Description for admins:	OFFICIAL-SENSITIVE sub-label
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Unticked
	Mark the content of files:	Ticked
Content marking	Add a header | Text:	OFFICIAL-SENSITIVE
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL-SENSITIVE
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black

Create a label step		Action
	Add a footer | Align text:	Center

Table 29 OFFICIAL-SENSITIVE | O-S EMBARGOED sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL-SENSITIVE - EMBARGOED
	Display name:	EMBARGOED
	Description for users:	This marking is applied to information that is only sensitive for a specific period and whose sensitivity will be reduced at the end of that period.
	Description for admins:	EMBARGOED for O-S
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-SENSITIVE-EMBARGOED-CO-OWNER@*tenantnamehere*	Co-Owner
	OFFICIAL-SENSITIVE-EMBARGOED-REVIEWER@*tenantnamehere*	Reviewer
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	OFFICIAL-SENSITIVE - EMBARGOED

Create a label step		Action
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL-SENSITIVE - EMBARGOED
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 30 OFFICIAL-SENSITIVE | O-S HMG USE ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL-SENSITIVE - HMG USE ONLY
	Display name:	HMG USE ONLY
	Description for users:	Applies to information that should only be shared with other HMG departments, and not with external partners.
	Description for admins:	HMG ONLY for O-S
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always

Create a label step		Action
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-SENSITIVE-HMG-ONLY-CO-AUTHOR@*tenantnamehere*	Co-Author
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	OFFICIAL-SENSITIVE - HMG USE ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL-SENSITIVE - HMG USE ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 31 OFFICIAL-SENSITIVE | O-S - OFFICIAL - [INSERT ORG] USE ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL-SENSITIVE – *[INSERT ORG]* USE ONLY
	Display name:	*[INSERT ORG] USE ONLY*
	Description for users:	Applies to information that should only be shared with the named organisation(s).
	Description for admins:	[INSERT ORG] USE ONLY for O-S
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected

Create a label step		Action
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-SENSITIVE-*ORG*-ONLY-CO-AUTHOR@*tenantnamehere*	Co-Author
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	OFFICIAL-SENSITIVE – *[INSERT ORG]* USE ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL-SENSITIVE – *[INSERT ORG]* USE ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 32 OFFICIAL-SENSITIVE | RECIPIENTS ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	OFFICIAL-SENSITIVE - RECIPIENTS ONLY
	Display name:	RECIPIENTS ONLY
	Description for users:	Indicates that the information must be handled on a strict need-to-know basis by select named individuals. Unauthorised sharing is not justified

Create a label step		Action
		due to the high risks associated with compromise.
	Description for admins:	RECIPIENTS ONLY for O-S
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails[4]:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Let users assign permissions when they apply the label
	In Outlook, enforce one of the following restrictions:	Do Not Forward
	In Word, PowerPoint and Excel, prompt users to specify permissions:	Ticked
Content marking	Add a header | Text:	OFFICIAL-SENSITIVE - RECIPIENTS ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	OFFICIAL-SENSITIVE - RECIPIENTS ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 33 UK OFFICIAL-SENSITIVE sensitivity parent label for content

[4] Refer to Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs for more details

Create a label step		Action
Name & description	Name:	UK OFFICIAL-SENSITIVE
	Display name:	UK OFFICIAL-SENSITIVE
	Description for users:	Applies to OFFICIAL information that is not intended for public release and could be of some interest to threat actors. A compromise is likely to cause moderate damage to the work or reputation of the organisation and/or HMG.
	Description for admins:	UK OFFICIAL-SENSITIVE parent label
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Unticked
	Mark the content of files:	Ticked
Content marking	Add a header | Text:	UK OFFICIAL-SENSITIVE
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL-SENSITIVE
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Create the remainder of these labels as sub-labels of the UK OFFICIAL-SENSITIVE parent label by clicking the three ellipsis and selecting the '+ Add sub label' option:

Table 34 UK OFFICIAL-SENSITIVE | O-S EMBARGOED sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL-SENSITIVE - EMBARGOED
	Display name:	EMBARGOED
	Description for users:	This marking is applied to information that is only sensitive for a specific period and whose sensitivity will be reduced at the end of that period.
	Description for admins:	EMBARGOED for UK O-S
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-SENSITIVE-EMBARGOED-CO-OWNER@*tenantnamehere*	Co-Owner
	OFFICIAL-SENSITIVE-EMBARGOED-REVIEWER@*tenantnamehere*	Reviewer
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	UK OFFICIAL-SENSITIVE - EMBARGOED
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center

Create a label step		Action
	Add a footer | Text:	UK OFFICIAL-SENSITIVE - EMBARGOED
	Add a footer | Font size:	Use your organisation’s default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 35 UK OFFICIAL-SENSITIVE | O-S HMG USE ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL-SENSITIVE HMG ONLY
	Display name:	HMG USE ONLY
	Description for users:	Applies to information that should only be shared with other HMG departments, and not with external partners.
	Description for admins:	HMG ONLY for UK O-S
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-SENSITIVE-HMG-ONLY-CO-AUTHOR@*tenantnamehere*	Co-Author

Create a label step		Action
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	UK OFFICIAL-SENSITIVE - HMG USE ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL-SENSITIVE - HMG USE ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 36 UK OFFICIAL-SENSITIVE | O-S - OFFICIAL - [INSERT ORG] USE ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL-SENSITIVE – *[INSERT ORG]* USE ONLY
	Display name:	*[INSERT ORG]* USE ONLY
	Description for users:	Applies to information that should only be shared with the named organisation(s).
	Description for admins:	*ORG*-ONLY for UK O-S
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Assign permissions now

Create a label step		Action
	User access to content expires:	Never
	Allow offline access:	Always
	Assign permissions to specific users and groups | Users and groups	Assign permissions | Permissions
	OFFICIAL-SENSITIVE-*ORG*-ONLY-CO-AUTHOR@*tenantnamehere*	Co-Author
	Use Double Key Encryption	Unticked
Content marking	Add a header | Text:	UK OFFICIAL-SENSITIVE – *[INSERT ORG]* USE ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL-SENSITIVE – *[INSERT ORG]* USE ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

Table 37 UK OFFICIAL-SENSITIVE | RECIPIENTS ONLY sensitivity sub-label for content

Create a label step		Action
Name & description	Name:	UK OFFICIAL-SENSITIVE - RECIPIENTS ONLY
	Display name:	RECIPIENTS ONLY
	Description for users:	Indicates that the information must be handled on a strict need-to-know basis by select named individuals. Unauthorised sharing is not justified

Create a label step		Action
		due to the high risks associated with compromise.
	Description for admins:	RECIPIENTS ONLY for UK O-S
Scope	Files & emails:	Ticked
	Groups & sites:	Unticked
Files & emails	Encrypt files and emails[5]:	Ticked
	Mark the content of files:	Ticked
Encryption	Configure encryption settings:	Selected
	Assign permissions now or let users decide:	Let users assign permissions when they apply the label
	In Outlook, enforce one of the following restrictions:	Do Not Forward
	In Word, PowerPoint and Excel, prompt users to specify permissions:	Ticked
Content marking	Add a header | Text:	UK OFFICIAL-SENSITIVE - RECIPIENTS ONLY
	Add a header | Font size:	Use your organisation's default
	Add a header | Font colour:	Black
	Add a header | Align text:	Center
	Add a footer | Text:	UK OFFICIAL-SENSITIVE - RECIPIENTS ONLY
	Add a footer | Font size:	Use your organisation's default
	Add a footer | Font colour:	Black
	Add a footer | Align text:	Center

[5] Refer to Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs for more details

OFFICIAL Container labels

The following tables, detail the recommended container sensitivity labels for UK public sector organisations.

> Note
>
> You may choose to implement additional container labels beyond the ones described below. The minimum recommended/required set are described in Table 38 below.
>
> The container labels have been intentionally designed to meet the different positive high-level outcomes they provide like making it clearer whether a container is intended for confidential internal use or collaboration with external guest users and/or external sharing enabled.
>
> Be careful when extending the recommended labels for example, community-based container labels, like an EXTERNAL - HMG ONLY container label, may sound like a simple win to enforce more control but enforcing this with sensitivity labels and CA is more complicated than it sounds and may not bring the benefits that were anticipated.
>
> If there is a need to provide more secure Microsoft Teams configuration refer to Configure a team with security isolation which described the configuration necessary to configure a team so that only team members can decrypt them.

The recommended container labels are INTERNAL – PUBLIC, INTERNAL - PRIVATE, EXTERNAL - PUBLIC, and EXTERNAL – PRIVATE, the list below provides more contextual guidance.

Internal – Public: for familiar/traditional Intranet style pages (such as HR and IT Services)

Internal – Private: for ORG USE ONLY-type workloads with internal invitees only and no external sharing

External – Public: for cases like "Visiting 70 Whitehall" sites that both internal and external users might find useful

External – Private: for most collaboration with Extranet style Sites and Teams with invited internal and external users

> Note
>
> Users/Owners can, via self-service or support ticket, change sensitivity label of a team after the initial application of the label. For example, "INTERNAL" teams that start out as an internal project/scope and then want to migrate to "EXTERNAL" to allow guest access and external sharing.

In the Microsoft Purview Information Protection portal, create each container label as a top-level label by clicking the '+ Create a label' option:

> Important
>
> The 'EXTERNAL-PUBLIC' container label should be placed with a priority that positions it above the OFFICIAL parent label but below the OFFICIAL-SENSITIVE parent label. This will ensure only content that is labelled as OFFICIAL can be stored within containers that have this label applied.

Table 38 EXTERNAL-PUBLIC sensitivity label for containers

Create a label step		Action
Name & description	Name:	EXTERNAL-PUBLIC
	Display name:	EXTERNAL-PUBLIC
	Description for users:	A workload container containing OFFICIAL data that is discoverable and accessible by all internal users and accessible by explicitly added external guests.
	Description for admins:	EXTERNAL-PUBLIC
Scope	Files & emails:	Unticked
	Groups & sites:	Ticked
Groups & sites	Privacy and external user access settings:	Ticked
	External sharing and Conditional Access settings:	Ticked
Privacy	Privacy:	Public
	External user access:	Ticked – let group owners add guests
External sharing & conditional access	Control external sharing from labelled SharePoint sites:	Ticked – New and existing guests
	Use Azure AD Conditional Access to protect labelled SharePoint sites:	Ticked
	Determine access:	Ticked
	Allow full access from desktop apps, mobile apps and the web:	Ticked

> Important
>
> The ‘EXTERNAL-PRIVATE’ container label should be placed with a priority that positions it above the OFFICIAL-SENSITIVE parent label but below the ‘INTERNAL-PRIVATE’ container label (that is created after this label). This will ensure content that is either OFFICIAL or OFFICIAL-SENSITIVE can be stored within containers that have this label applied.

Table 39 EXTERNAL-PRIVATE sensitivity label for containers

Create a label step		Action
Name & description	Name:	EXTERNAL-PRIVATE
	Display name:	EXTERNAL-PRIVATE
	Description for users:	For workload containers only accessible to internal and external named individuals/users. This includes persistent Guest access and ad-hoc/one-off file sharing by link.
	Description for admins:	EXTERNAL-PRIVATE
Scope	Files & emails:	Unticked
	Groups & sites:	Ticked
Groups & sites	Privacy and external user access settings:	Ticked
	External sharing and Conditional Access settings:	Ticked
Privacy	Privacy:	Private
	External user access:	Ticked – let group owners add guests
External sharing & conditional access	Control external sharing from labelled SharePoint sites:	Ticked – New and existing guests
	Use Azure AD Conditional Access to protect labelled SharePoint sites:	Ticked
	Determine access:	Ticked
	Allow full access from desktop apps, mobile apps and the web:	Ticked

> Important
>
> The 'INTERNAL-PUBLIC' container label should be placed with a priority that positions it above the 'EXTERNAL-PRIVATE' container label. This will ensure content that is either OFFICIAL or OFFICIAL-SENSITIVE can be stored within containers that have this label applied.

Table 40 INTERNAL-PUBLIC sensitivity label for containers

Create a label step		Action
Name & description	Name:	INTERNAL-PUBLIC
	Display name:	INTERNAL-PUBLIC
	Description for users:	For containers storing data that should only be accessed by members of your organisation/users inside your organisation/your employees/your staff.
	Description for admins:	INTERNAL-PUBLIC
Scope	Files & emails:	Unticked
	Groups & sites:	Ticked
Groups & sites	Privacy and external user access settings:	Ticked
	External sharing and Conditional Access settings:	Ticked
Privacy	Privacy:	Public
	External user access:	Unticked – no external access
External sharing & conditional access	Control external sharing from labelled SharePoint sites:	Ticked – Only people in your organisation
	Use Azure AD Conditional Access to protect labelled SharePoint sites:	Ticked
	Determine access:	Ticked
	Allow full access from desktop apps, mobile apps and the web:	Ticked

> Important
>
> The 'INTERNAL-PRIVATE' and 'INTERNAL-PUBLIC' container label should be placed with a priority that positions it above the 'EXTERNAL-PRIVATE' container label. This will ensure content that is either OFFICIAL or OFFICIAL-SENSITIVE can be stored within containers that have this label applied.

Table 41 INTERNAL-PRIVATE sensitivity label for containers

Create a label step		Action
Name & description	Name:	INTERNAL-PRIVATE
	Display name:	INTERNAL-PRIVATE
	Description for users:	For containers storing data that should only be accessed by members of your organisation/users inside your organisation/your employees/your staff.
	Description for admins:	INTERNAL-PRIVATE
Scope	Files & emails:	Unticked
	Groups & sites:	Ticked
Groups & sites	Privacy and external user access settings:	Ticked
	External sharing and Conditional Access settings:	Ticked
Privacy	Privacy:	Private
	External user access:	Unticked – no external access
External sharing & conditional access	Control external sharing from labelled SharePoint sites:	Ticked – Only people in your organisation
	Use Azure AD Conditional Access to protect labelled SharePoint sites:	Ticked
	Determine access:	Ticked
	Allow full access from desktop apps, mobile apps and the web:	Ticked

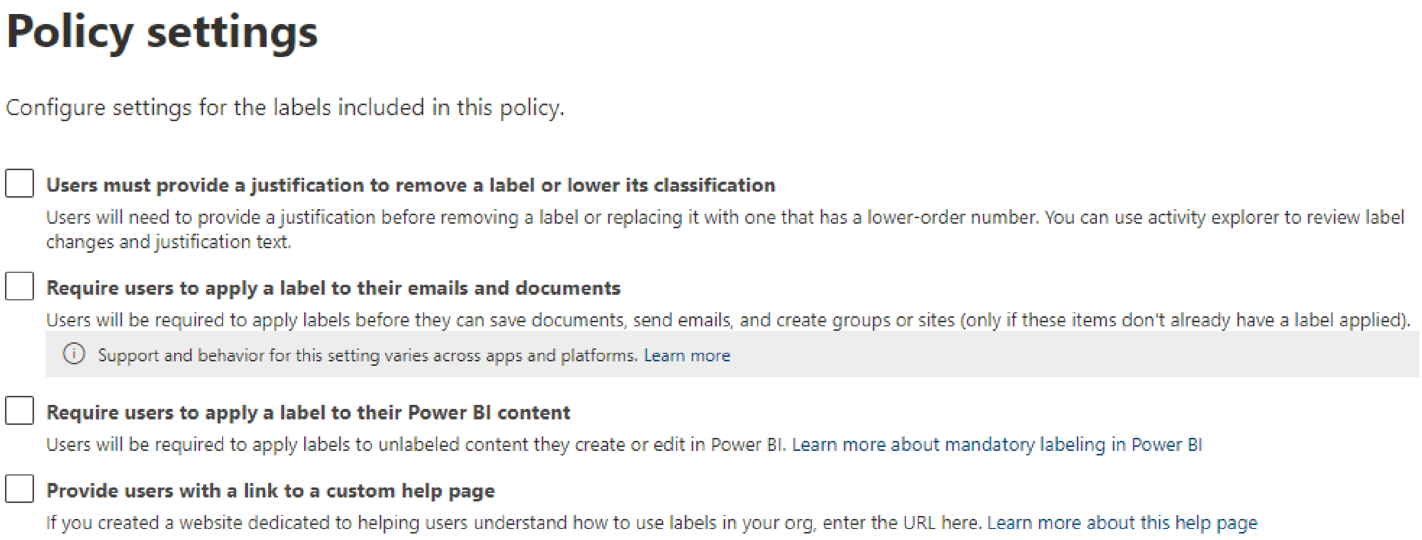
5.3.1.2 Publish sensitivity labels

To publish sensitivity labels, browse to the Microsoft 365 compliance center portal. Navigate to Information protection | Label policies and click the 'Publish label' button.

Follow the wizard to publish sensitivity labels.

You will need to provide the following data:

- Which labels to publish.
- A mail-enabled AzureAD security group to publish the label to.
- Decide on answers to the following questions:



Policy settings

Configure settings for the labels included in this policy.

☐ **Users must provide a justification to remove a label or lower its classification**
Users will need to provide a justification before removing a label or replacing it with one that has a lower-order number. You can use activity explorer to review label changes and justification text.

☐ **Require users to apply a label to their emails and documents**
Users will be required to apply labels before they can save documents, send emails, and create groups or sites (only if these items don't already have a label applied).
ⓘ Support and behavior for this setting varies across apps and platforms. Learn more

☐ **Require users to apply a label to their Power BI content**
Users will be required to apply labels to unlabeled content they create or edit in Power BI. Learn more about mandatory labeling in Power BI

☐ **Provide users with a link to a custom help page**
If you created a website dedicated to helping users understand how to use labels in your org, enter the URL here. Learn more about this help page

Figure 11: Policy settings

- Whether to set default labels for documents and/or emails.
- Publishing policy name and description.

For more info, visit the following page: Publish sensitivity labels by creating a label policy

To publish content labels use the following information.

> ### Important
>
> If your organisation has added additional labels or modified the label names, ensure that they are selected as part of the labels to publish for the pilot.

Table 42 UK GOV OFFICIAL POLICY FOR CONTENT sensitivity label publishing policy

Publish label step		Action
Choose sensitivity labels to publish	Sensitivity labels to publish:	Select all the labels created for the pilot
Publish to users and groups	Users & groups:	Initially to your pilot user group: 'UK GOV Classification Pilot' After successfully completing your pilot, publish the labels to All users using: 'UK GOV Classification'
Policy settings	Users must provide a justification to remove a label or lower its classification:	Ticked
	Require users to apply a label to their emails and documents:	Ticked

Publish label step		Action
	Require users to apply a label to their Power BI content:	Ticked
	Provide users with a link to a custom help page:	Unticked – unless you have already prepared a taxonomy webpage, in which case tick this option and provide the relevant URL
Apply a default label to documents	Apply this default label to documents:	None
Apply a default label to emails	Apply this default label to emails:	Same as document
	Require users to apply a label to their emails:	Ticked
Name your policy	Name:	UK GOV OFFICIAL POLICY FOR CONTENT
	Enter a description for your sensitivity label policy:	This policy publishes the common set of content sensitivity labels required to operate at the UK GOVERNMENT OFFICIAL DATA TIERING.

To publish container labels, use the following information.

Table 43 UK GOV OFFICIAL POLICY FOR CONTAINERS sensitivity label publishing policy

Publish label step		Action
Choose sensitivity labels to publish	Sensitivity labels to publish:	Select all the labels created for the pilot
Publish to users and groups	Users & groups:	Initially to your pilot user group: 'UK GOV Classification Pilot' After successfully completing your pilot, publish the labels to All users using: 'UK GOV Classification'
Policy settings	Users must provide a justification to remove a label or lower its classification:	Ticked

Publish label step		Action
	Require users to apply a label to their emails and documents:	Ticked
	Require users to apply a label to their Power BI content:	Ticked
	Provide users with a link to a custom help page:	Unticked – unless you have already prepared a taxonomy webpage, in which case tick this option and provide the relevant URL
Apply a default label to documents	Apply this default label to documents:	None
Apply a default label to emails	Apply this default label to emails:	Same as document
	Require users to apply a label to their emails:	Ticked
Name your policy	Name:	UK GOV OFFICIAL POLICY FOR CONTAINERS
	Enter a description for your sensitivity label policy:	This policy publishes the common set of workload container sensitivity labels required to operate at the UK Government OFFICIAL Security Classification

After successfully completing the labels pilot, create a duplicate set of the above labels and policies, that will be published to the entire org using the UK GOV Classification group.

> Note: You need to retain the pilot labels for the next phase of piloting, which includes encryption.
>
> Do not publish the pilot labels to the wider organisation. At this point the pilot users will see two sets of what appear to be the same labels, but one set will soon be modified to enable the encryption pilot as explained in the next section of this guide.

5.3.2 Encryption pilot

The encryption pilot is used to determine the impact of enabling encryption on sensitivity labels and how it interacts with other security products your organisation uses, specifically email gateways, anti-virus products and 3rd party DLP products. The intent of this pilot is to minimise the potential disruption that enabling encryption may introduce, but this requires that your pilot user group is a representative subset of your entire organisation to allow issues to be identified and acted upon accordingly.

To initiate the pilot, associate the UK GOV Classification Pilot group with the Content Encryption labels to associate the pilot users group with labels that have encryption enabled.

It's worth remembering that encrypted emails or documents will prevent collaboration with external organisations that are not brought into the pilot groups using their external guest collaboration accounts. For more info on configuring external guest collaboration, refer to the Cross Gov Collaboration guide.

The approach for the encrypted labels pilot is to create a duplicate set of labels that are assigned to the pilot user group, validate that encryption does not impact the organisations email gateway, anti-virus product or 3rd party DLP tool before updating the production label templates to include the encryption settings in the label.

The encryption labels pilot will have the biggest impact on the pilot users as emails and documents that have the pilot label applied will need to be updated to the production sensitivity labels that include encryption, after the pilot has been successfully completed. To determine which content has been encrypted with the pilot encryption sensitivity labels, use the Compliance Content Explorer tool to search and locate these. Then work with the corresponding pilot users to adjust to the production sensitivity labels and replace all instances of the pilot encryption labels.

After successfully completing the encryption labels pilot assign UK GOV Classification group to the Content Labels to publish the content labels to the organisation. Leave the UK GOV Classification Pilot group associated to ensure that they retain the label assignment.

5.3.3 Data Loss Prevention (DLP) pilot

It is recommended to use Data Loss Prevention (DLP) rules to provide guard rails around the handling of sensitive data in emails, Teams, SharePoint and OneDrive. Microsoft's future development is now focussed on DLP as a method to provide these controls. Organisations who have been using Exchange (EXO) Mail Flow/Transport Rules (MFR) should migrate to the equivalent functionality provided by DLP rules. Refer to Data loss prevention in Exchange Online Migrating from Exchange Transport Rules to Unified DLP - The complete playbook - Microsoft Tech Community and How DLP works with Security & Compliance Center & Exchange admin center - Microsoft 365 Compliance | Microsoft Docs

Data Loss Prevention rules provide a way for organisations to prevent their users from inappropriately sharing sensitive data with people who should not have access to the information.

Key points for how DLP compliments MPIP are described below:

- DLP can prevent sharing of files vs. sensitivity labels, which can just prevent access (through rights management) if shared via email; or a guest user, for example, who has access to a site for some reason, won't be able to see a file that meets a certain condition.
- Combine DLP with the use of sensitivity labels - DLP might not find anything sensitive in your document based on its native rules, but it doesn't mean that the content isn't sensitive (unless your write a custom REGEX DLP for every possible situation which isn't likely). So DLP might not block it as it doesn't match any of the native DLP rules, or your 5 custom REGEX rules, but the content might still be sensitive which will still be protected by a sensitivity label that your users apply.

> Important
>
> It is recommended to create separate Data Loss Prevention (DLP) policies for each Microsoft 365 workload to gain the most functionality. It is possible to create DLP policies that combine workloads, but if you do this you lose certain settings that can only be applied when an individual workload is selected, refer to When creating DLP policies, consider separate policies per workload

In the use case shown in Figure 12 below, DLP is used to identify a document or email containing a health record and then automatically prevents external sharing of that document (or blocks the email from being sent) and notifies the recipient with "policy tips"; and an alert is sent to the end-user and admin.

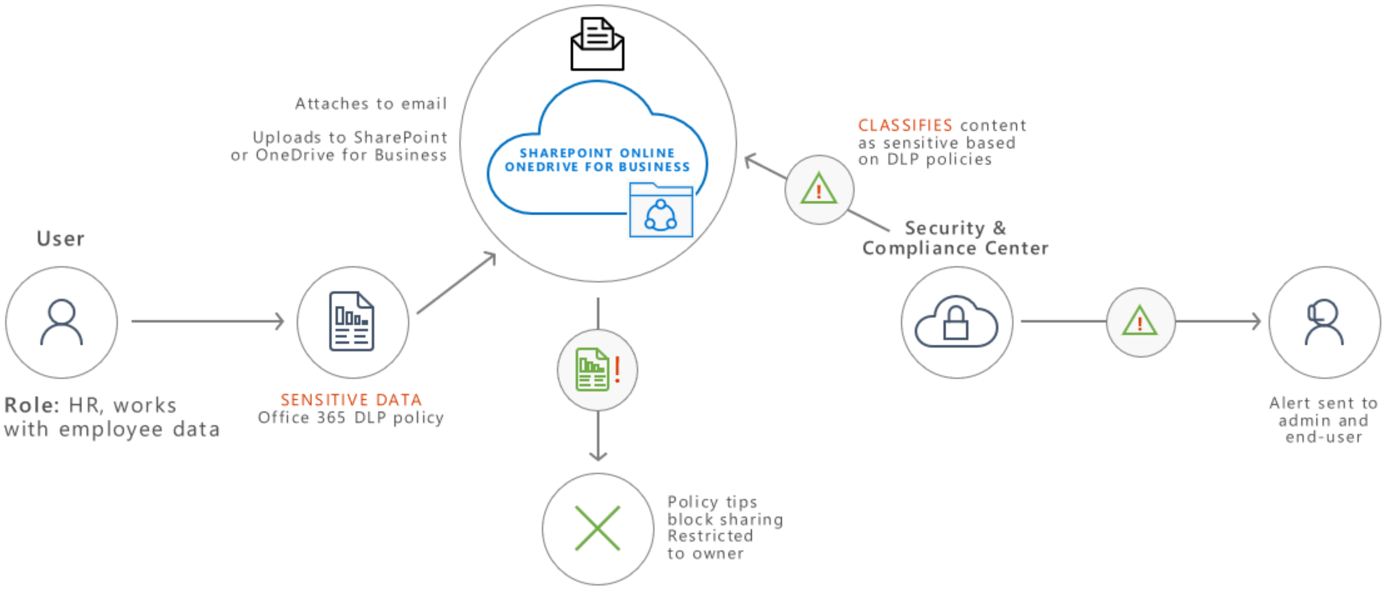

Attaches to email
Uploads to SharePoint or OneDrive for Business
SHAREPOINT ONLINE ONEDRIVE FOR BUSINESS
CLASSIFIES content as sensitive based on DLP policies
Security & Compliance Center
User
Role: HR, works with employee data
SENSITIVE DATA Office 365 DLP policy
Alert sent to admin and end-user
Policy tips block sharing Restricted to owner

Figure 12: Example use case for protecting personal data using DLP

For more info, visit the following page: Learn about data loss prevention

5.3.3.1 DLP for email

ORG-only

The following steps enable a DLP rule for Exchange Online (EXO) email to prevent content that has the 'OFFICIAL - *HMG* USE ONLY' label applied from being sent externally (i.e. outside the organisation) but allowed to be sent internally (to full members of staff inside the organisation). Repeat these steps for the 'O-S - *HMG USE* ONLY' label (replace the references to the 'OFFICIAL - *HMG USE* ONLY' label) to create a separate DLP policy.

> Note
>
> Replace *ORG* with your organisation name.

Table 44: DLP for email policy creation steps

DLP policy step	Action
Navigate to the Microsoft 365 Compliance portal | Data loss prevention | Policies blade	Click the '+ Create policy' link
On the 'Start with a template or create a custom policy' wizard page	Select Custom (under 'Categories') and Custom policy (under 'Templates'), then click Next
On the 'Name your DLP policy' wizard page	Provide a suitable name and description for the DLP policy – use the following as an example: 'Block external email for OFFICIAL - *ORG* USE ONLY', then click Next

DLP policy step	Action
On the 'Choose locations to apply the policy' wizard page	De-select all options, apart from Exchange email. Then determine which groups should be included and excluded for the policy. As an example, leave the default (which includes all users and excludes no users). Then click Next
On the 'Define policy settings' wizard page	Leave the defaults (Create or customize advanced DLP rules) and click Next
On the 'Customize advanced DLP rules' wizard page	Click the '+ Create rule' link
On the 'Create rule' wizard page	Provide the information as described in Table 26: DLP rule items, that follows below

Table 45: DLP rule items

DLP rule item		Action
Name		Block external email for OFFICIAL - ORG USE ONLY rule
Description		Blocks email from being sent externally when the 'OFFICIAL - ORG-ONLY' label is applied
Conditions	Content is shared from Microsoft 365 AND Content contains	with people outside my organisation Sensitivity labels OFFICIAL/ORG USE ONLY
Actions	Restrict access or encrypt the content in Microsoft 365 locations	Block users from receiving email or accessing shared SharePoint, OneDrive and Teams files. Block only people outside your organization
User notifications	On	Notify users in Microsoft 365 service with a policy tip Notify the user who sent, shared, or last modified the content.
Incident reports	Severity	High On Send alert every time an activity matches the rule Use email incident reports to notify you when a policy match occurs Send notifications to these people: *NameOfAlertsSharedMailbox*
	All incident reports include information about the item that was matched, where the match occurred, and the rules and	The name of the person who last modified the content: Ticked The types of sensitive content that matched the rule: Ticked The rule's severity level: Ticked

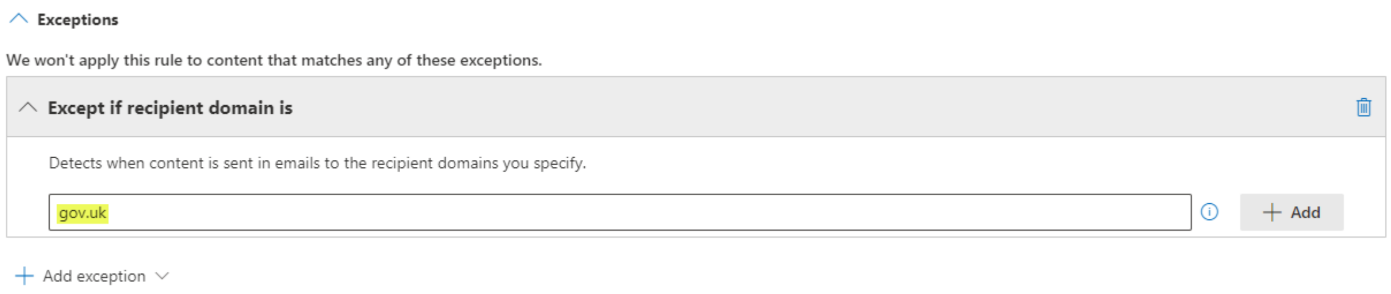
DLP rule item		Action
	policies it triggered. You can also include the following information in the report:	The content that matched the rule, including the surrounding text: Ticked The item containing the content that matched the rule: Ticked
Additional options	If there's a match for this rule, stop processing additional DLP policies and rules	Ticked Priority 0

Table 46: DLP for email policy creation steps continued

DLP policy step	Action
On the 'Create rule' wizard page	Once you have completed the rule items, then click Save and Next
On the 'Test or turn on the policy' wizard page	Decide whether you are comfortable in turning it on right away or test it out first. It is recommended to test first – but remember that in test mode nothing is blocked, it is only logged that it would have been blocked. You can always edit the policy to switch the policy on later, after verifying in test mode first. Then click Next
On the 'Review your policy and create it' wizard page	Click Submit
On the 'New policy created' wizard page	Click Done

HMG-ONLY

For the HMG Only label – repeat the above 'ORG USE ONLY' DLP for email steps – but select the OFFICIAL – HMG USE ONLY label and add an exception if recipient domain is gov.uk (and any additional email domains that should be allowed):



Exceptions

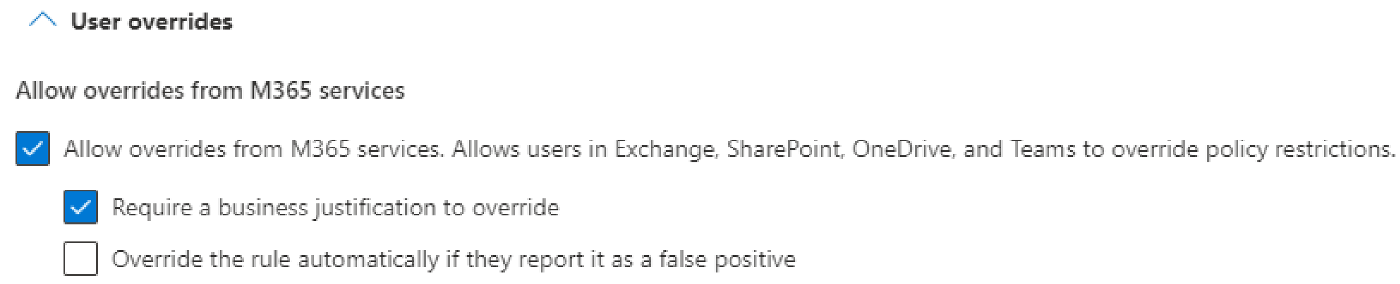
We won't apply this rule to content that matches any of these exceptions.

Except if recipient domain is

Detects when content is sent in emails to the recipient domains you specify.

gov.uk

Enabling user override with a required business justification is recommended for the HMG-ONLY DLP rule for email. This means that users are not prevented from doing their job if they need it, but the organisation still has an audit of this activity and can investigate as necessary.



^ **User overrides**

Allow overrides from M365 services

☑ Allow overrides from M365 services. Allows users in Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

☑ Require a business justification to override

□ Override the rule automatically if they report it as a false positive

5.3.4 Conditional Access pilot

Conditional Access is at the heart of the new identity driven control plane. Conditional Access is a feature used to bring signals together, to make decisions, and enforce organisational policies. Conditional Access is at the heart of Microsoft's Zero Trust security model and the identity driven control plane that provides the coarse-grained authorisation to cloud applications like Microsoft Teams and SharePoint Online.

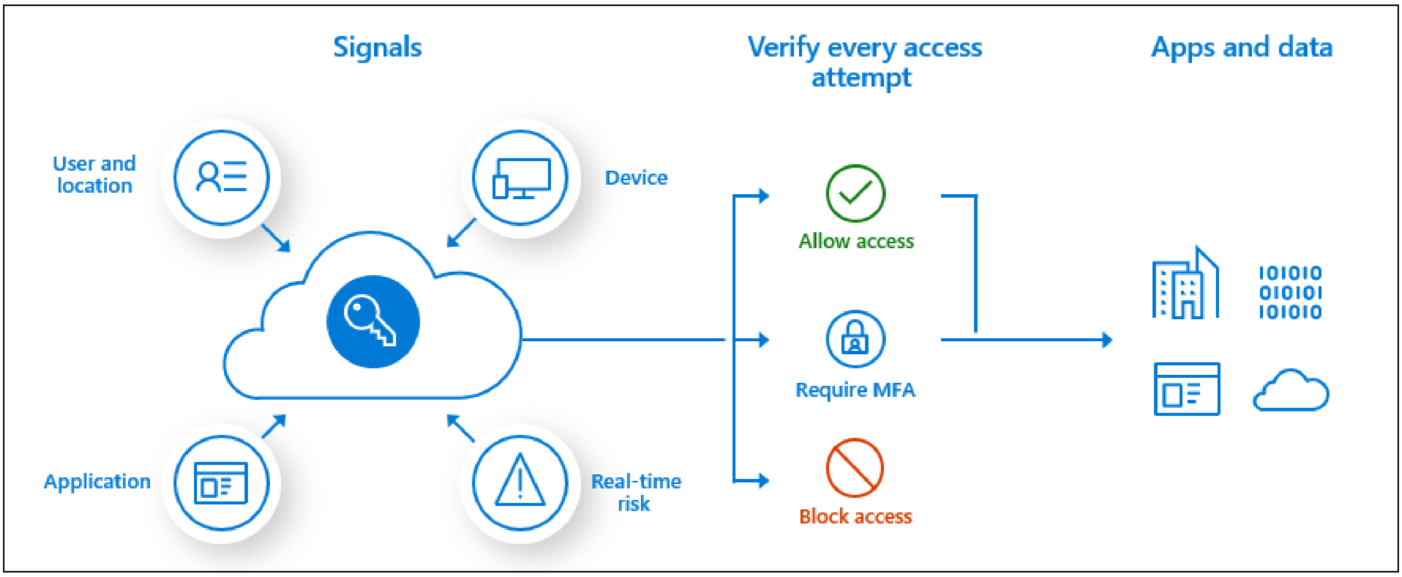


Figure 13: Conditional Access decision-based authorisation

Figure 13 Conditional Access decision-based authorisation described the components that make up Conditional Access, details of the signals that are used by conditional access are described in more detail here

Integrating MPIP into Conditional Access means more fine-grained access decisions can be made than with just MPIP. You can improve access policies by combining existing signals, including the identity of the user and device being used, with the sensitivity of the resource being accessed.

The recommended Conditional Access policies are described in Microsoft 365 Guidance for UK Government: Secure Configuration Blueprint

5.3.4.1 Cross-tenant access settings – trusted external organisations

Prior to Cross-tenant access settings Conditional Access could not use information about the device being used by a guest user. This meant organisations were only able to require MFA to gain confidence in the user's identity and nothing about the device being used. This is why the BYOD Guidance for UK OFFICIAL recommends that access to OFFICIAL data from BYOD or a device with no verifiable assertion should use Office Web Apps to access content (files) or workload containers (Microsoft Teams, SharePoint) content.

Now, with Cross-tenant access settings organisations can include the device compliance status as part of Conditional Access policy evaluation for external guest access which introduces the potential for a new externally managed device type. This may give you sufficient confidence that desktop apps on partners compliant devices can be used to access OFFICIAL content (files) or workload containers (Microsoft Teams, SharePoint) content rather than forcing the use of the web-apps only.

As described in Figure 14 Cross-tenant access settings and MPIP combined give even finer control of what can and cannot be done by users outside of your organisation but within trusted partner organisations such as other government organisations.

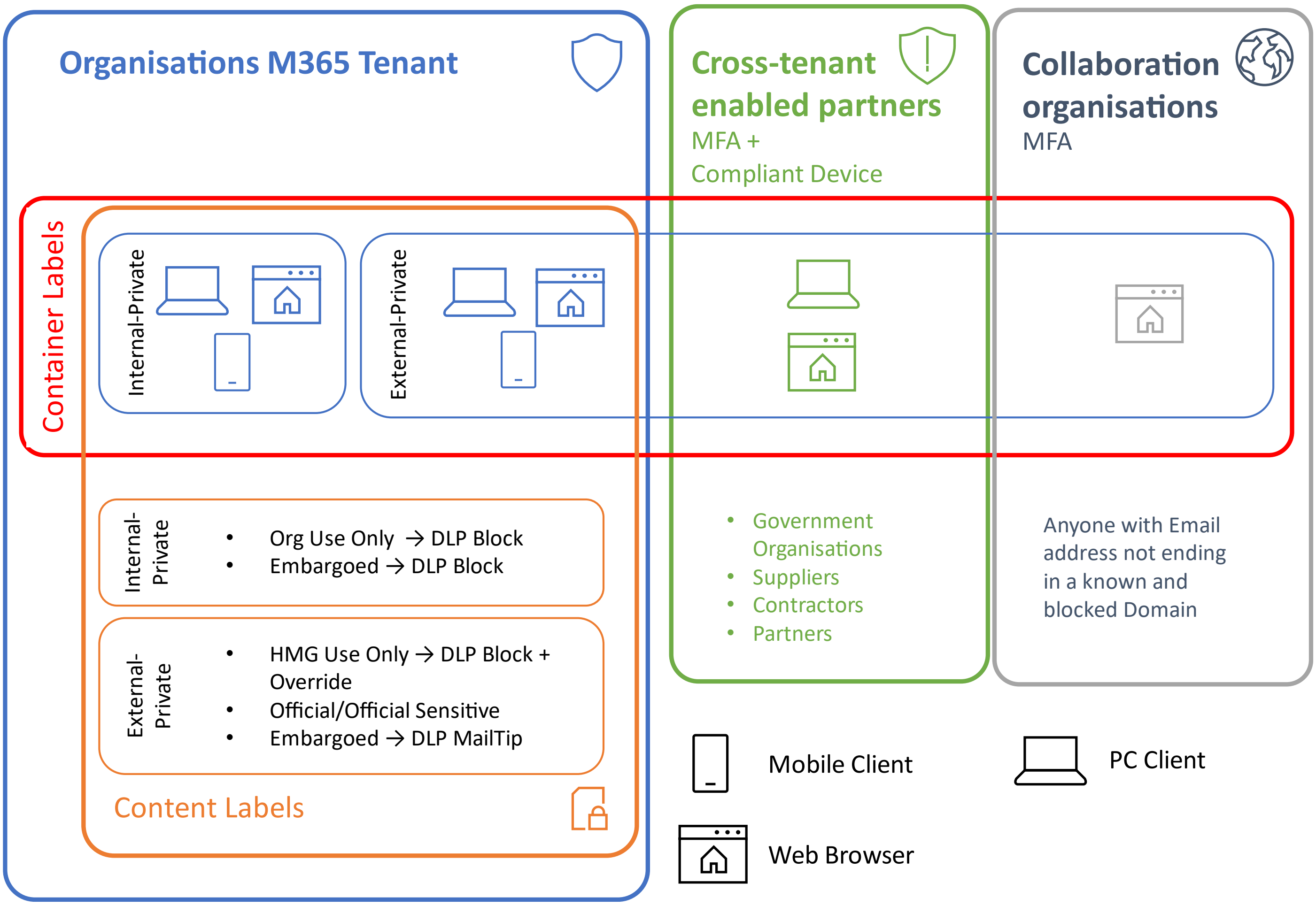

Organisations M365 Tenant
Cross-tenant enabled partners
MFA +
Compliant Device
Collaboration organisations
MFA
Container Labels
Internal-Private
External-Private
Internal-Private
• Org Use Only → DLP Block
• Embargoed → DLP Block
External-Private
• HMG Use Only → DLP Block + Override
• Official/Official Sensitive
• Embargoed → DLP MailTip
Content Labels
• Government Organisations
• Suppliers
• Contractors
• Partners
Anyone with Email address not ending in a known and blocked Domain
Mobile Client
PC Client
Web Browser

Figure 14: Office Application platform based on Device Assurance

Table 47 Definition of device trust types describes how external managed devices provide a mechanism to raise security posture by presenting additional claims during the Conditional Access policy evaluation.

Table 47: Definition of device trust types

Device Type	Definition
Corporate Managed PC	Trusted device as it is centrally managed by organisation and aligns to the platform specific NCSC End User Device Security Guidance for the device
Corporate Managed Mobile	Trusted device as it is centrally managed by organisation and aligns to the platform specific NCSC End User Device Security Guidance for the device
External Managed PC	Trusted if the device can present device Hybrid Azure AD Joined or Compliant device claim from an explicitly trusted external partner using Cross-tenant access policies/settings.

External Managed Mobile	Trusted if the device can present device compliant device claim from an explicitly trusted external partner using Cross-tenant access policies/settings.
BYOD Mobile	Guest mobile device with no verifiable assertion about the device health or compliance

> **Information**
>
> If your organisation's risk appetite is such that allowing OFFICIAL-SENSITIVE content being opened in desktop app on an externally managed device is not acceptable, then utilise a Conditional Access policy to only allow web-apps to be used for OFFICIAL-SENSITIVE marked content. Refer to Microsoft 365 UK Blueprint - Secure Configuration Alignment document for details on how to configure Conditional Access and Microsoft 365 workloads to support this. For organisations that have Microsoft E5 Security or Microsoft 365 E5 licenses refer to Section 6.1.1 later in this document.

Refer to Cross-tenant access with Azure AD External Identities for more information and for more specific information on how Cross-tenant access settings form part of the Cross Government Collaboration Guidance refer to the Strategy document and supporting Technical guide

5.4 Run Phase

The last stage is about optimizing the solution for Microsoft 365. This phase introduces mandatory labelling across the organisation. Also in this phase, you will set up an automated scalable approach for each solution. Keep monitoring the results and fine tune the rules. Validate the results through alerts/reports and take the appropriate actions.

The following controls are included in the Run phase:

Add Table 48 49: Run phase

Control	Action
Hide the encrypt and do not forward buttons in Microsoft 365	Consider hiding encrypt (and do not forward) button in Office – use sensitivity label version instead. Refer to section 5.4.2 Hide encrypt and do not forward
Sensitive Information Types (SITs)	Start thinking about SITs - work with your pilot users to understand common keywords used by their departments. Refer to Section 5.4.5 Tools to help with Sensitive Information Types (SITs) testing
Client-side sensitivity label auto-labelling in Microsoft 365 Apps (Microsoft 365 ProPlus/Business client apps), Office for the Web, and Office Mobile based on sensitive information types	Use the Microsoft 365 compliance center to create and edit sensitivity labels. During the label creation/editing wizard, select the option to enable auto-labelling for files and emails. Provide the required label matching conditions. Auto-labelling can be configured to either recommend a label (allowing the user to accept or decline the recommendation) or automatically apply a label (once you are confident enough with the accuracy of the detection process). Refer to Section 5.4.3 Apply sensitivity labels automatically in Microsoft 365 Apps
Server-side sensitivity label auto-labelling for files in SharePoint	Turn audit log search on Enable sensitivity labels for Office files in SharePoint and OneDrive

Control	Action
Online (SPO) or exchange Online (EXO) email	Use the Microsoft 365 compliance center Auto-labelling to apply the relevant label that matches the conditions you specify. Refer to Section 5.4.4 Apply sensitivity labels automatically in SharePoint and Exchange online

5.4.1 Enable mandatory labelling across organisation

Once the label pilot phases have been successfully completed in the Walk phase, to complete the implementation of the sensitivity labels the 'Require users to apply a label to their emails and documents' option in your sensitivity label policy must be set to ticked to force mandatory labelling.

5.4.2 Hide encrypt and do not forward

Once fully implemented (so after piloting is completed and the sensitivity labels are enabled with encryption), the HMG ONLY, ORG ONLY and EMBARGOED (for both the OFFICIAL and OFFICIAL-SENSITIVE) sensitivity labels described in this guide will enforce encryption.

The OFFICIAL-SENSITIVE - RECIPIENTS ONLY sensitivity label described in this guide enforces 'Do Not Forward' in Outlook.

When the Do Not Forward option is applied to an email, the email is encrypted, and recipients must be authenticated. Then, the recipients cannot forward it, print it, or copy from it. For example, in the Outlook client, the Forward button is not available, the Save As and Print menu options are not available, and you cannot add or change recipients in the To, Cc, or Bcc boxes.

Unprotected Office documents that are attached to the email automatically inherit the same restrictions. The usage rights applied to these documents are Edit Content, Edit; Save; View, Open, Read; and Allow Macros. If different usage rights are required for an attachment, or the attachment is not an Office document that supports this inherited protection, the file must be protected before attaching it to the email. Then assign the specific usage rights needed for the file.

By default, the full Outlook client application and Outlook web access show Encrypt and Do Not Forward buttons in their ribbon toolbar. This is not part of the Microsoft Purview Information Protection toolset and can be confusing to end-users. It is recommended to remove these options, to ensure your users can only operate by using sensitivity labels to control sharing behaviours.

Follow these instructions to hide the buttons.

For the full Outlook client application:

Create a PowerShell script that you deploy to your client devices. The script should run the following commands:

```
if((Test-Path -LiteralPath "HKCU:\SOFTWARE\Microsoft\Office\16.0\Common\DRM") -ne $true) { New-Item "HKCU:\SOFTWARE\Microsoft\Office\16.0\Common\DRM" -force -ea SilentlyContinue };

New-ItemProperty -LiteralPath 'HKCU:\SOFTWARE\Microsoft\Office\16.0\Common\DRM' -Name 'DisableEO' -Value 1 -PropertyType DWord -Force -ea SilentlyContinue;

New-ItemProperty -LiteralPath 'HKCU:\SOFTWARE\Microsoft\Office\16.0\Common\DRM' -Name 'DefaultPermissionTemplateGuid' -Value 'irmdnf' -PropertyType String -Force -ea SilentlyContinue;

New-ItemProperty -LiteralPath 'HKCU:\SOFTWARE\Microsoft\Office\16.0\Common\DRM' -Name 'DisableDNF' -Value 1 -PropertyType DWord -Force -ea SilentlyContinue;
```

For Outlook web access:

The following PowerShell commands should be run from a Privileged Access Workstation (with access to your environment) that has the latest version of the ExchangeOnlineManagement module installed:

```
Connect-ExchangeOnline
```

Then authenticate using an account that has administrative privileges for Exchange Online.

```
Set-IRMConfiguration -SimplifiedClientAccessEnabled $false -
SimplifiedClientAccessDoNotForwardDisabled $true -SimplifiedClientAccessEncryptOnlyDisabled
$true
```

Although this hides the Encrypt option, there's also a 'Set Permissions' menu options in the ellipsis that can be hidden with this PowerShell command:

```
Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -IRMEnabled $false
```

Once you have deployed these changes, the 'Encrypt-Only' and 'Do Not Forward' options will be disabled under the Encrypt button in the Microsoft 365 ribbon toolbar:

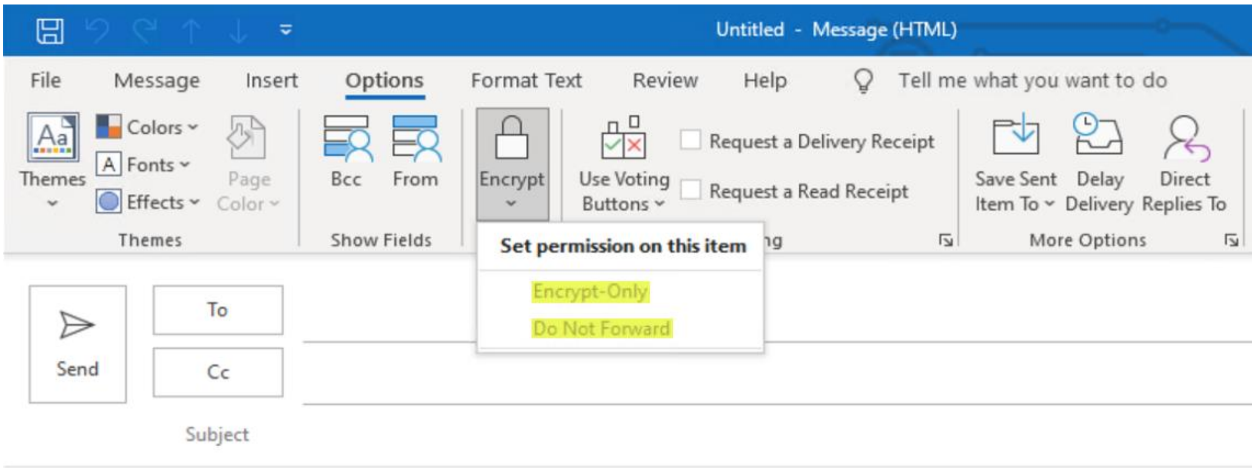


Figure 15: Encrypt and Do Not Forward options disabled

For more info visit the following page: Disabling the Encrypt-Only feature in Outlook

5.4.3 Apply sensitivity labels automatically in Microsoft 365 Apps

Client-side labelling supports recommending a label to users, as well as automatically applying a label. But in both cases, the user decides whether to accept or reject the label, to help ensure the correct labelling of content. This client-side labelling has minimal delay for documents because the label can be applied even before the document is saved.

An administrator determines which data requires labelling by defining Sensitive Info Types (SITs). A SIT is a pre-defined list of keywords that the system looks for in the data. When a match is found, the system can either automatically apply a label or prompt the user to alert them which label is recommended to be applied.

For more info, visit the following page: How to configure auto-labeling for Office apps

5.4.4 Apply sensitivity labels automatically in SharePoint and Exchange online

This approach to auto-labelling is configured using the service-side model. This applies a sensitivity label to data at rest, residing in SharePoint, OneDrive, Teams and Exchange.

Because this labelling is applied by services rather than by applications, you don't need to worry about what apps users have and what version. As a result, this capability is immediately available throughout your organization and suitable for labelling at scale. Auto-labelling policies don't support recommended labelling because the user doesn't interact with the labelling process. Instead, the administrator runs the policies in simulation to help ensure the correct labelling of content before applying the label.

5.4.5 Tools to help with Sensitive Information Types (SITs) testing

When testing SITs and Endpoint DLP actions, it can be useful to have a library of links to assist in this testing:

- https://filebin.net – excellent for testing HTTP post/upload actions
- https://dlptest.com – provides several testing options as well as samples for common restricted items such as credit card numbers, SSN, etc.
- https://fauxid.com/ - Provides you with data that can be used to generate SSN, credit card numbers etc.

For more info, visit the following page: How to configure auto-labelling policies for SharePoint, OneDrive, and Exchange

6 Enhanced capabilities

The configuration implemented in the Walk & Run phases requires mostly Microsoft E3 licensing. The features and capabilities described in this section require Microsoft 365 E5 or Microsoft 365 E5 Compliance and build upon the previously implemented capabilities to allow further automation of labelling, more granular control for web sessions, and more sophisticated DLP capability for endpoints.

6.1 Enhanced Conditional Access capabilities

6.1.1 Conditional Access Session Control with Microsoft Defender for Cloud Apps (MDCA)

For organisations whose risk appetite requires that they need additional controls to further reduce their attack surface, guest users can be forced to use a web browser to access to Teams, SharePoint sites and files. Additional control can be achieved using Conditional Access policies that integrate with Microsoft Defender for Cloud Apps (MDCA) to provide a reverse proxy architecture. The capability enforces access controls on your organization's apps based on certain conditions. The conditions define which users, Microsoft 365 applications and devices a Conditional Access policy applies to. After you've determined the appropriate conditions, Microsoft 365 traffic is brokered through MDCA where Conditional Access App Control protects your data by applying access and session controls.

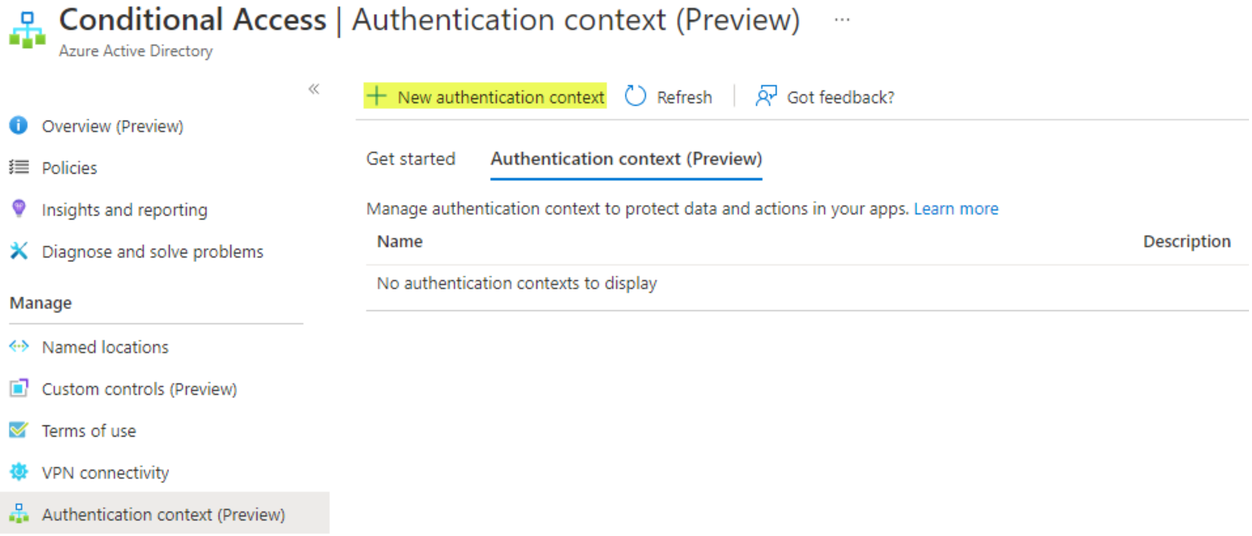
For workload containers, this is done with an Azure AD Conditional Access session control policy. MDCA session control policies allow you to restrict external guest users to accessing your corporate Microsoft 365 data from inside a browser. This enables you to enforce additional controls, such as:

- Monitor all activities to provide audit events of when a user accesses a document and whether they attempted to print it.
- Block all downloads preventing users from downloading files to their device allowing files only to be viewed in Web Browser.
- Block specific activities by preventing guest users from being able to print documents.
- Require step-up authentication (authentication context) to require a user is prompted to MFA before they can access documents.
- Protect files on download enforce encryption of files by applying the appropriate Sensitivity Label before they are downloaded
- Protect uploads of sensitive files to cloud storage services that are not approved by your organisation.

6.1.2 Authentication context

A recently added Azure AD feature: Authentication Context extends the capabilities of Conditional Access and sensitivity labels for workload containers. Once these are defined, an authentication context can be applied by using a sensitivity label to provide granular control over who can access the data inside the container. So, this means apps like SharePoint will require additional information (like a user completing an MFA challenge or being required to connect from a managed device) to gain access to a document that is stored there. Refer to Authentication context for more detailed information.

To enable this feature, first requires you to define an authentication context. Navigate to the Azure portal (Azure Active Directory | Protect & Secure | Conditional Access | Authentication context) and click the '+ New authentication context' button:



Conditional Access | Authentication context (Preview)

Azure Active Directory

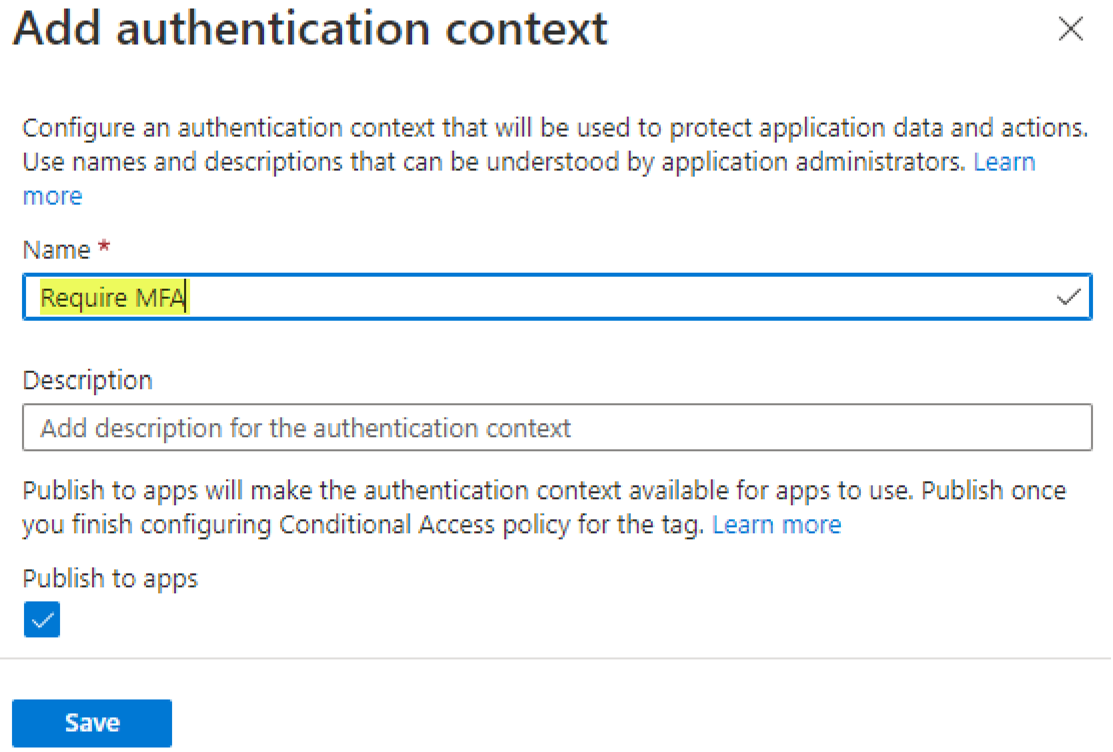
Overview (Preview)
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication context (Preview)
+ New authentication context
Refresh
Got feedback?
Get started
Authentication context (Preview)

Manage authentication context to protect data and actions in your apps. Learn more

Name	Description
No authentication contexts to display	

Figure 16: Conditional Access – New authentication context

Provide a name (and a description if required) for the new authentication context and click the Save button (making sure the 'Publish to apps' box is checked):



Add authentication context

Configure an authentication context that will be used to protect application data and actions. Use names and descriptions that can be understood by application administrators. Learn more

Name *

Require MFA

Description

Add description for the authentication context

Publish to apps will make the authentication context available for apps to use. Publish once you finish configuring Conditional Access policy for the tag. Learn more

Publish to apps

☑

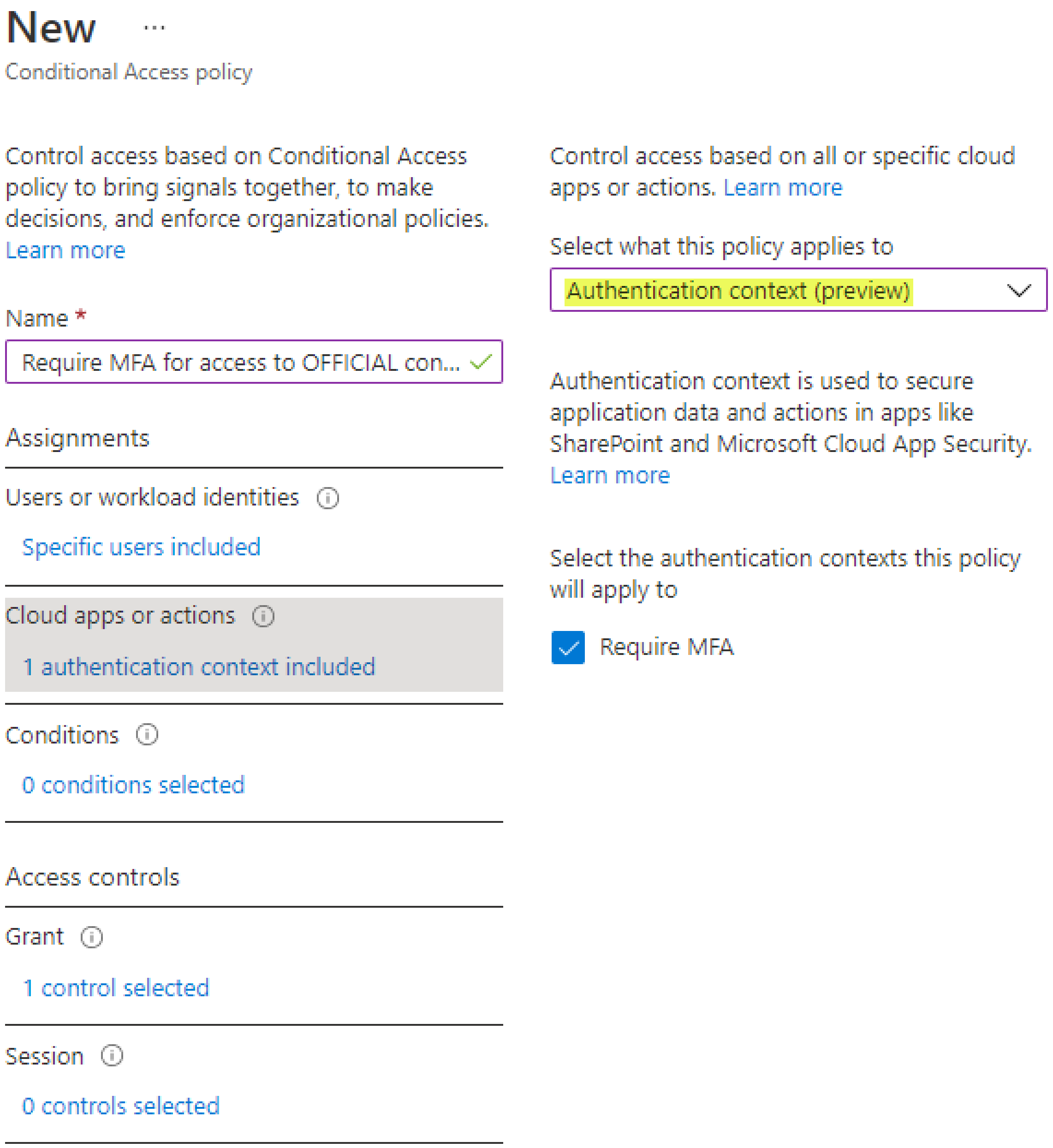
Figure 17: Conditional Access – Add authentication context

By ensuring that the 'Publish to apps' checkbox is enabled, this means that this authentication context is visible to apps like sensitivity labels and can be used by Conditional Access policies.

The next step is to create a new Conditional Access policy to take advantage of the authentication context. The following policy requires the user to successfully complete an MFA challenge before they can access the content that is marked with the associated sensitivity label.

Setting	Action
Assignments	
Name:	Require MFA for access to OFFICIAL-SENSITIVE content
Users and groups:	*Target the appropriate Azure AD group of users*
Cloud apps or actions	
Select what this policy applies to:	Authentication context (preview)
Select the authentication contexts this policy will apply to:	Require MFA
Conditions:	–
Access controls	
Grant:	Require multi-factor authentication
Session:	–

Table 50 Conditional Access policy – authentication context



New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Require MFA for access to OFFICIAL con... ✓

Assignments

Users or workload identities ⓘ

Specific users included

Cloud apps or actions ⓘ

1 authentication context included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Control access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to

Authentication context (preview)

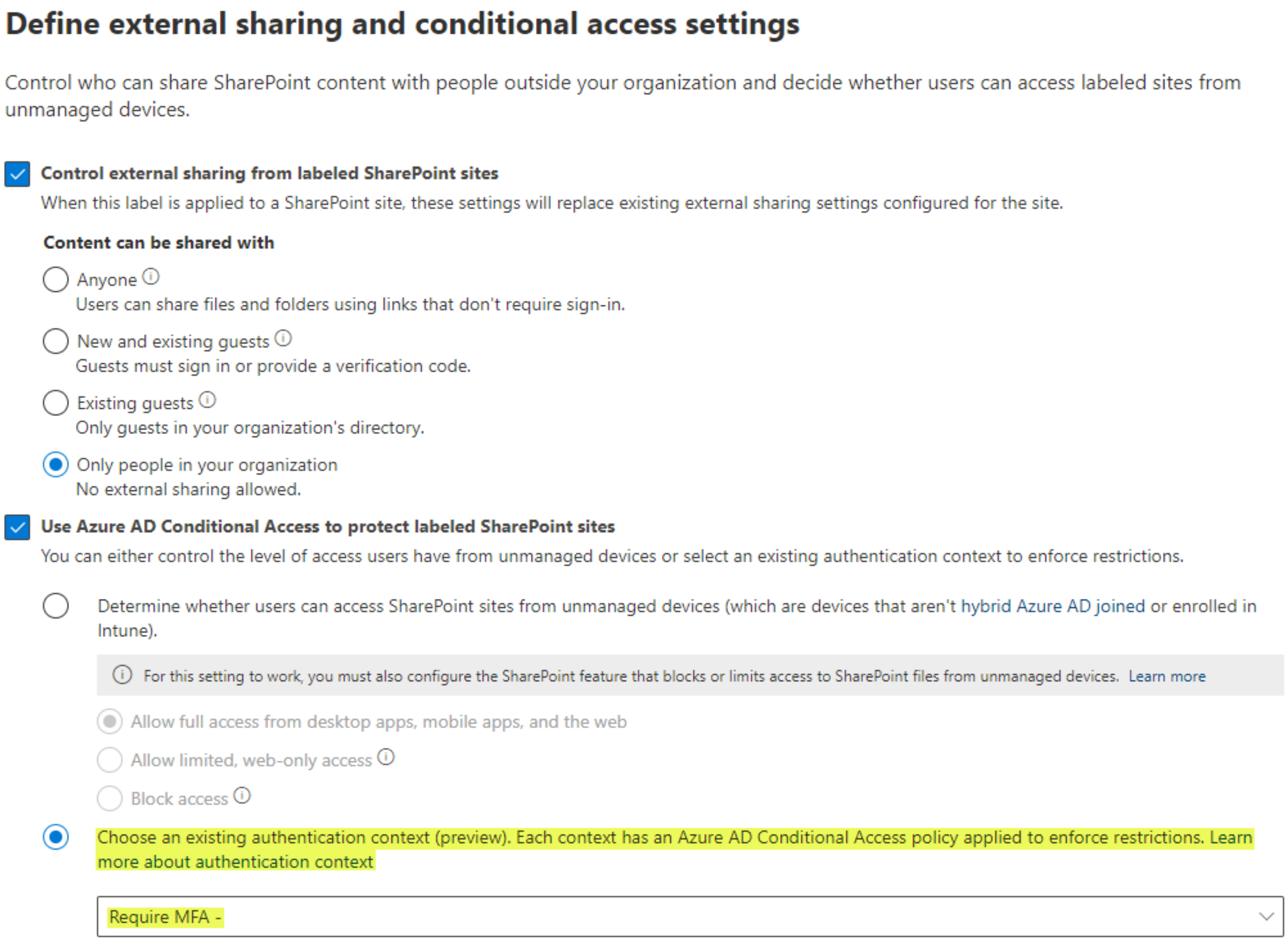
Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security. Learn more

Select the authentication contexts this policy will apply to

☑ Require MFA

Figure 18: Conditional Access – new authentication context policy requiring MFA

Finally, create a workload container sensitivity label (or update an existing one) and use the ‘Define external sharing and conditional access settings’ page to enable the authentication context setting:



Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

☑ **Control external sharing from labeled SharePoint sites**
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

○ Anyone ⓘ
Users can share files and folders using links that don't require sign-in.

○ New and existing guests ⓘ
Guests must sign in or provide a verification code.

○ Existing guests ⓘ
Only guests in your organization's directory.

● Only people in your organization
No external sharing allowed.

☑ **Use Azure AD Conditional Access to protect labeled SharePoint sites**
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

○ Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't hybrid Azure AD joined or enrolled in Intune).

ⓘ For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. Learn more

● Allow full access from desktop apps, mobile apps, and the web

○ Allow limited, web-only access ⓘ

○ Block access ⓘ

● Choose an existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions. Learn more about authentication context

Require MFA -

Figure 19: Sensitivity label – require authentication context

When a user attempts to access a site with the authentication context label applied, SharePoint Online contacts Azure AD to locate the associated Conditional Access policy. This is then invoked, which (using the above example) will require the user to successfully pass the MFA challenge to access the data.

For more information, please visit the following page: Cloud apps, actions, and authentication context in Conditional Access policy

6.2 Data Loss Reduction using Microsoft Defender for Cloud Apps (MDCA)

Visibility of data is important since it is difficult to protect what you don’t know exists. Organisations store data in many different areas using different cloud storage providers. With Microsoft 365 you have OneDrive for Business for personal storage and SharePoint Online for enterprise storage.

Organisations may also be using third-party cloud storage providers, like Box, Dropbox, AWS or Google Workspace, to diversify their repositories or may be in the process of migration to a single repository within the Microsoft cloud. In either case the ability to see sensitive content and protect it is always high on the priority list when it comes to security. Incorporating MDCA gives you visibility, dynamic alerting and the ability to take actions against specific scenarios through policies for connected cloud applications beyond just data residing in Microsoft 365.

MDCA has file governance capabilities to monitor and protect data stored in your Software-as-a-Service (SaaS) cloud applications. There are various methods to connect your cloud apps using features such as Cloud-to-Cloud integration, API connectors, or real-time access and session controls.

Once an app is connected, protection is provided by a built-in anomaly detection engine. Additionally, visibility into the app's user and device activities becomes possible. This enables control over what data is shared by the app, by building detection policies with governance to mitigate any risky activities or sensitive-data sharing by the app.

MDCA policies can be used to enforce several scenarios (such as discovering shadow IT, detecting suspicious user activity and blocking downloads of sensitive information) but for this guidance the ability to use DLP for sensitive content shared publicly is the specific use case to support data loss reduction.

The following link describes a recommended approach to getting started with discovering data in your cloud apps and how to manage it: Discover and protect sensitive information in your organization tutorial | Microsoft Docs

6.3 Further DLP enhancements

Additional Data Loss Prevention features can be enabled to further enhance the protections and controls in your environment.

6.3.1 Reducing sharing of Documents marked as Organisation Only externally

To help educate and inform users when they attempt to share documents that have the OFFICIAL or OFFICIAL-SENSITIVE - Organisation Only label applied a DLP Policy that is scoped to SharePoint and OneDrive workloads is used.

This is done by building a DLP policy to block sharing of files with OFFICIAL or OFFICIAL-SENSITIVE - Organisation Only label and notify the user that they need to change the label before they can share this. This should be combined and scoped to sites that allow for external sharing.

Refer to Preventing and educating users from sharing sensitive documents externally

6.3.2 Prevent sharing until DLP has processed content

When new files are added to SharePoint or OneDrive in Microsoft 365, it may take a few moments for them to be crawled and indexed. It takes additional time for the Office Data Loss Prevention (DLP) policy to scan the content and apply rules to help protect sensitive information. If external sharing is turned on, sensitive content could be shared and accessed by guests before the Office DLP rule finishes processing. You can ensure that documents are protected until DLP scans and marks them as safe to share using a PowerShell cmdlet to enable a feature called Sensitive by Default:

```
Set-SPOTenant -MarkNewFilesSensitiveByDefault BlockExternalSharing
```

For more information, visit the following page: Mark new files as sensitive by default

6.4 Endpoint DLP

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on your managed devices. Once devices are onboarded into the Microsoft

365 compliance solutions, the information about what users are doing with sensitive items is made visible in Activity Explorer and you can enforce protective actions on those items via DLP policies.

Endpoint DLP can be used to prevent users from accidently or maliciously uploading sensitivity labelled content to their personal cloud storage location or USB storage device.

> Note
>
> When working with Endpoint DLP, be aware that content is evaluated when created or modified. Existing content at rest on the device is not scanned at this time.

For more info, visit the following page: Get started with Endpoint data loss prevention

For additional refer to Section 6.2.3 in Microsoft 365 UK Blueprint

> Information
>
> Endpoint DLP is only applicable to managed devices therefore Conditional Access and MDCA session controls are used to provide similar capability.

6.5 Configure SharePoint default document templates

To help with the use of the correct label, one approach that can be used is to create document templates that are pre-configured with the appropriate label. These can then be published for data originators to make use of.

Additional pieces of information can also be pre-staged into these document templates. For example – custom text descriptors that are stored in the header or footer. Or specific pieces of meta-data that are written into the document properties. The use of such additional data can be helpful when defining custom Sensitive Information Types (SITs) – by improving the confidence of a successful match by adding these items to the keyword dictionaries that the SITs use to discover and match sensitive data.

To make it easier for data originators to consume these document templates, SharePoint can be configured to host these by making use of Site content types. Data originators can then create new documents in a SharePoint site that are based on these pre-defined templates.

To create a custom content type in SharePoint Online to support the labelling taxonomy refer to the following links, Create a content type and Create an organization assets library will allow users to select the templates from desktop apps and not just when in SharePoint site.

6.6 Web Application experience

One of the key features of Microsoft 365 Office web apps is the ability to use labels to manage and organize documents, making collaboration and information management more efficient. However, when editing documents through a browser, users might encounter some limitations, such as not being able to see the label marking in the header or footer. This feature is only visible when printing, viewing the header or footer, or when in viewing mode.

To work around this limitation, users can switch to viewing mode to see the label markings in the header or footer. By doing so, they can verify the correct placement and formatting of the labels. Moreover, when printing the document, the label markings will be displayed, ensuring that the final output aligns with the users' expectations. Users can also access the header or footer directly to inspect and modify the label markings as needed.

7 Recommended training

To learn about all of the Microsoft Compliance tools in detail, visit the following webpage for links to the Ninja training series: All the Microsoft Ninja Training I Know About

8 Summary

This document has focussed on labelling documents and emails in Microsoft 365, but Microsoft Purview is capable of much more to help organisations to improving their risk and compliance posture. Microsoft Purview is not just one feature it is a framework, a suite of products, that work together to provide visualization of sensitive data, lifecycle protection for data, and data loss prevention.

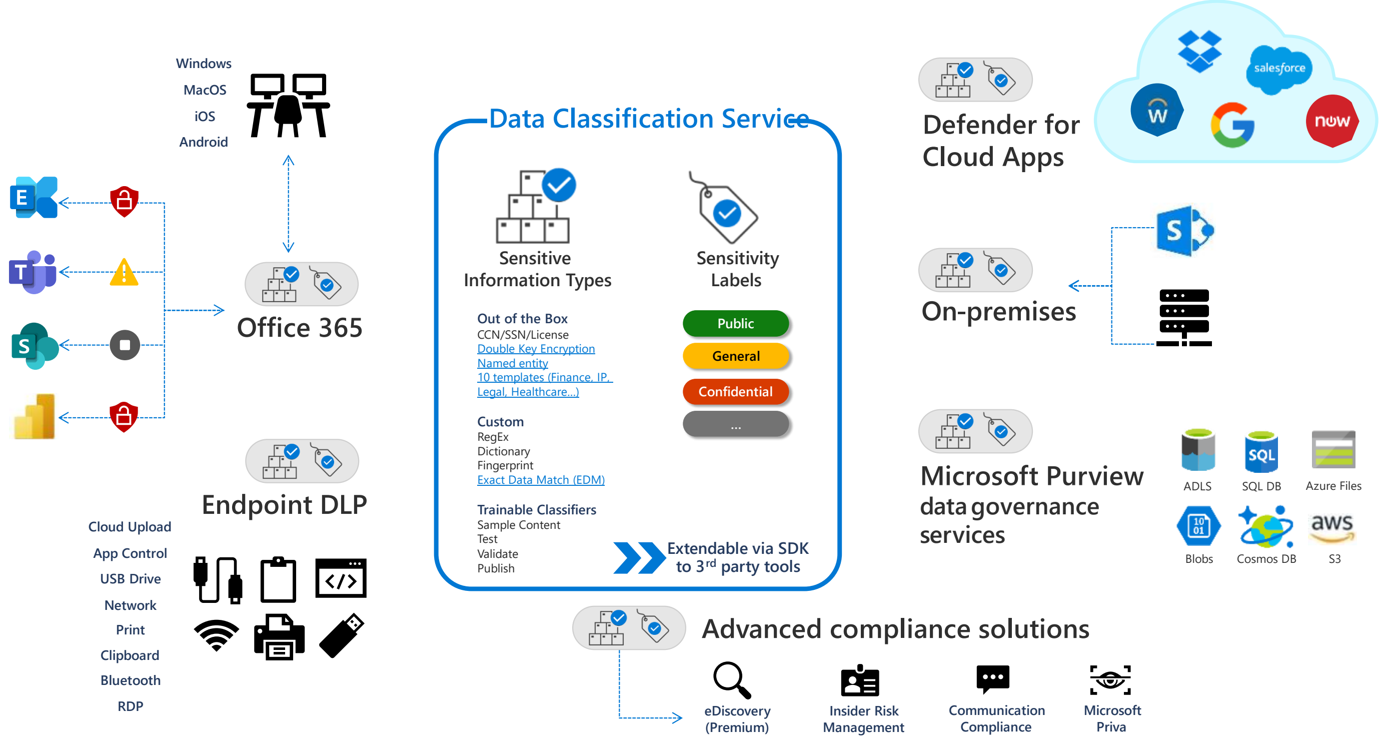


Figure 20: Microsoft Purview overview

In addition to our native integration, we are equally committed to ensuring our customers and partners can integrate these same capabilities directly within their own line-of-business applications and solutions.

This includes our Information Protection SDK, as well as a rich set of extensible Graph APIs that are available to ISVs, MSSPs, and system integrators to use.

Learn more about Microsoft Purview Information Protection from our webpage and get a deeper view of Microsoft Purview Information Protection from our tech docs: aka.ms/MIPdocs

Contact Customer Support Account Manager (CSAM) to explore how MPIP can help protect other data in your organisation.

9 Appendix A: Supporting configuration

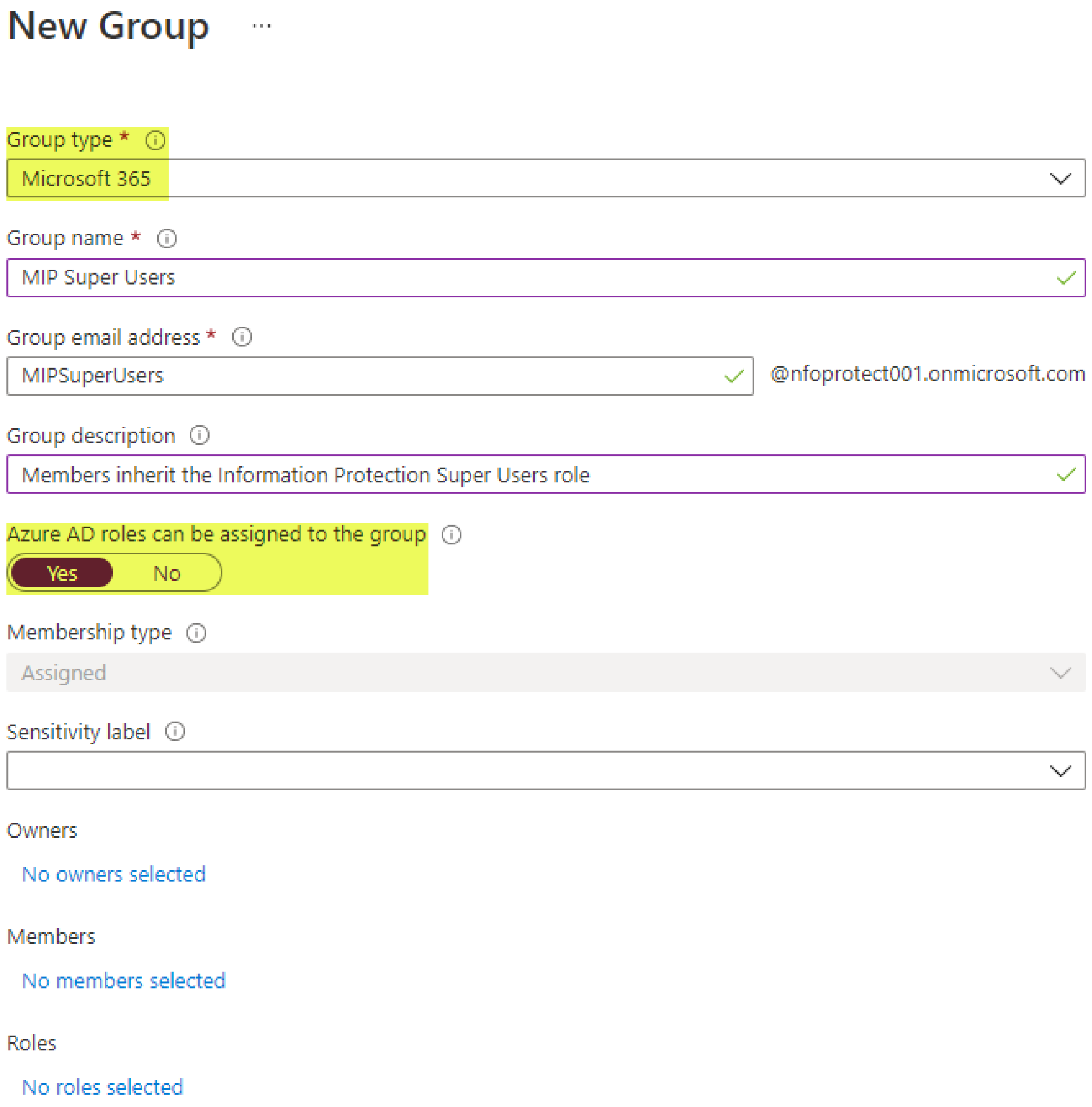
This section describes items for additional consideration.

9.1 Create Super User Privileged Access Group

This section describes the detailed steps required to create the Super User Privileged Access group.

To configure the PIM eligible super user role, follow these instructions.

1. Open the Azure portal and navigate to Azure Active Directory | Groups and click the New group button
2. On the New Group blade, click the 'Yes' button below the 'Azure AD roles can be assigned to the group' option and change the Group type to 'Microsoft 365'. Then provide suitable information for the Group name ('MPIP Super Users' in the following screenshot) and Group description ('Members inherit the Information Protection Super Users role' in the following screenshot). Your blade should look like the following screenshot (note the highlighted changes you must select):



New Group ...

Group type * ⓘ
Microsoft 365

Group name * ⓘ
MIP Super Users ✓

Group email address * ⓘ
MIPSuperUsers ✓ @nfoprotect001.onmicrosoft.com

Group description ⓘ
Members inherit the Information Protection Super Users role ✓

Azure AD roles can be assigned to the group ⓘ
[✓ Yes] No

Membership type ⓘ
Assigned

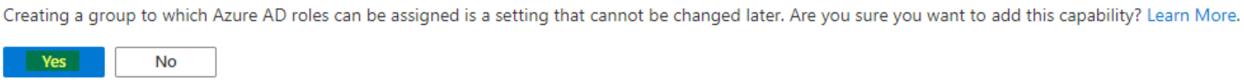
Sensitivity label ⓘ

Owners
No owners selected

Members
No members selected

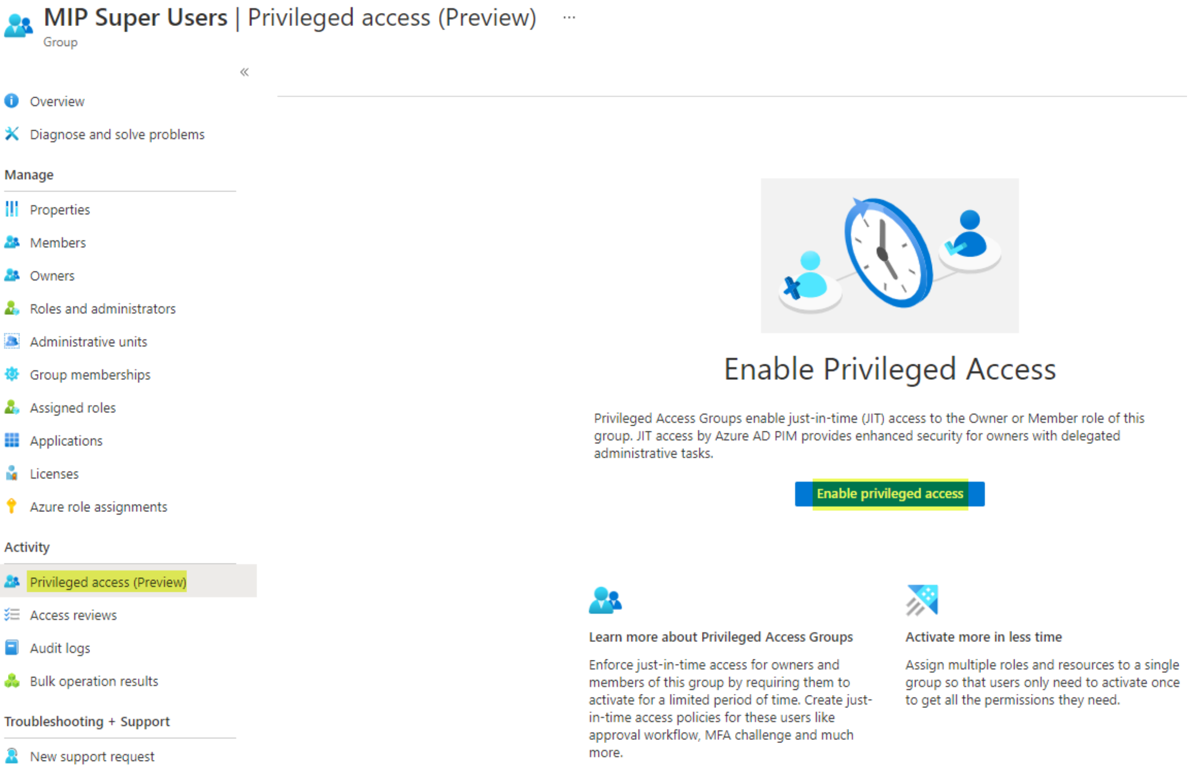
Roles
No roles selected

3. Agree to the message that warns you about making this group role-enabled by clicking the 'Yes' button:



Creating a group to which Azure AD roles can be assigned is a setting that cannot be changed later. Are you sure you want to add this capability? Learn More.

4. Once the group has been created, select it from the list of groups shown in the Azure AD All Groups portal. Then click the Privileged access (Preview) button (shown under the 'Activity' section) and then click the Enable privileged access button:



MIP Super Users | Privileged access (Preview)

Enable Privileged Access

Privileged Access Groups enable just-in-time (JIT) access to the Owner or Member role of this group. JIT access by Azure AD PIM provides enhanced security for owners with delegated administrative tasks.

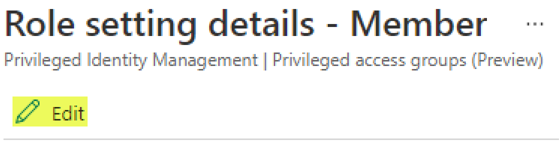
Learn more about Privileged Access Groups

Enforce just-in-time access for owners and members of this group by requiring them to activate for a limited period of time. Create just-in-time access policies for these users like approval workflow, MFA challenge and much more.

Activate more in less time

Assign multiple roles and resources to a single group so that users only need to activate once to get all the permissions they need.

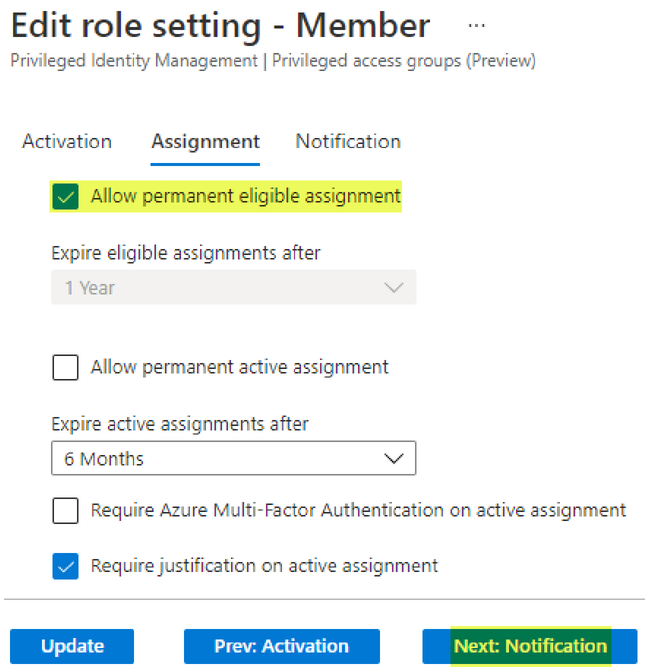
5. Click the 'Settings' button and then select 'Member'. On the 'Role settings details – Member' blade, click the Edit button:



Role setting details - Member

Privileged Identity Management | Privileged access groups (Preview)

6. Adjust the 'Activation maximum duration (hours)' setting down to 4 (or lower if appropriate for your environment). You can adjust the other settings on this page according to your requirements, otherwise leave them at the default and click the 'Next: Assignment' button at the bottom.
7. Select the 'Allow permanent eligible assignment' setting and click the 'Next: Notification' button at the bottom:



Edit role setting - Member ···

Privileged Identity Management | Privileged access groups (Preview)

☑ Allow permanent eligible assignment

Expire eligible assignments after: 1 Year

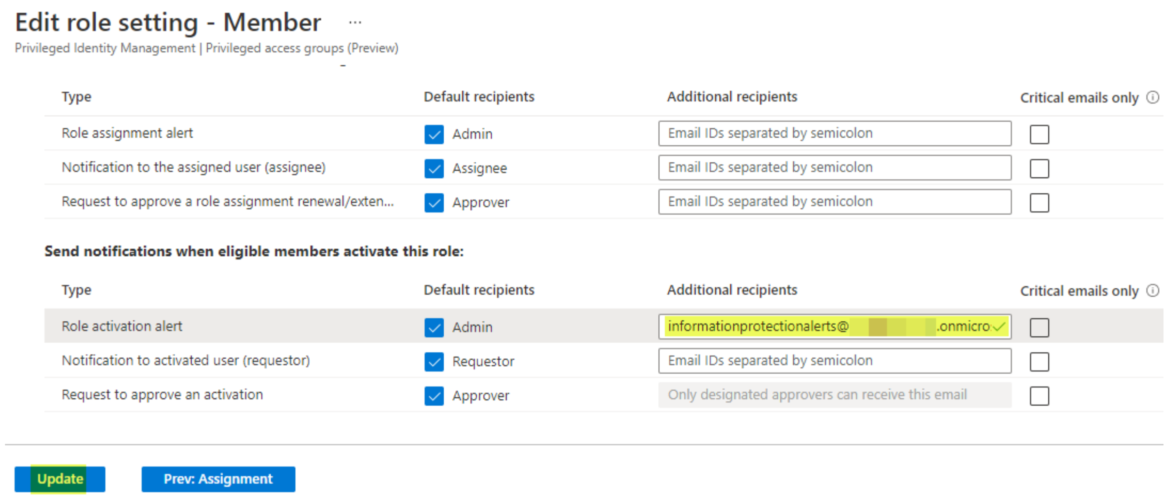
□ Allow permanent active assignment

Expire active assignments after: 6 Months

□ Require Azure Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

8. Under the ‘Send notifications when eligible members activate this role:’ section, enter the email address for the Information Protection notification shared mailbox, then click the Update button:



Edit role setting - Member ···

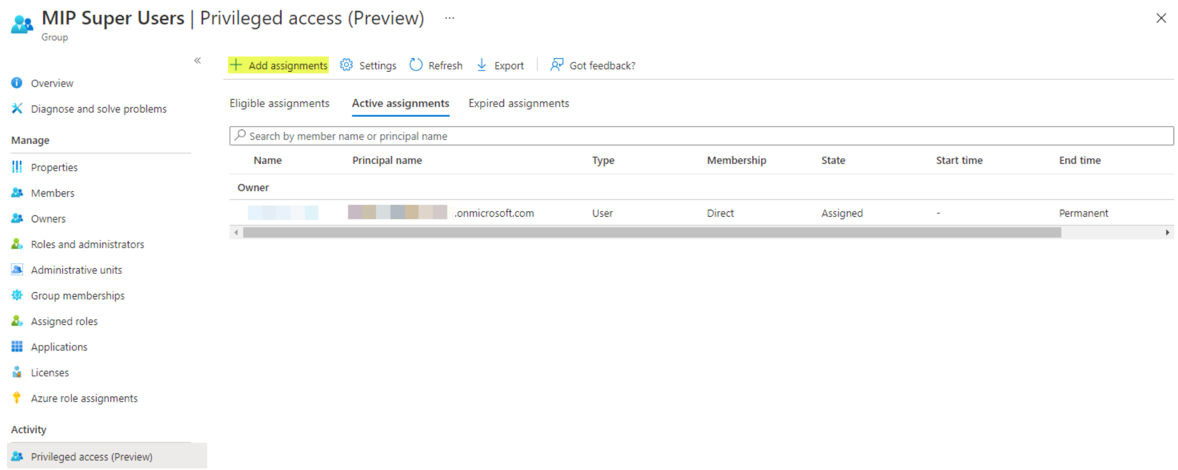
Privileged Identity Management | Privileged access groups (Preview)

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	☑ Admin	Email IDs separated by semicolon	□
Notification to the assigned user (assignee)	☑ Assignee	Email IDs separated by semicolon	□
Request to approve a role assignment renewal/exten...	☑ Approver	Email IDs separated by semicolon	□

Send notifications when eligible members activate this role:

Type	Default recipients	Additional recipients	Critical emails only
Role activation alert	☑ Admin	informationprotectionalerts@[redacted].onmicro ✓	□
Notification to activated user (requestor)	☑ Requestor	Email IDs separated by semicolon	□
Request to approve an activation	☑ Approver	Only designated approvers can receive this email	□

9. Return to the Privileged access (Preview) blade and then click the ‘+ Add assignments’ button:

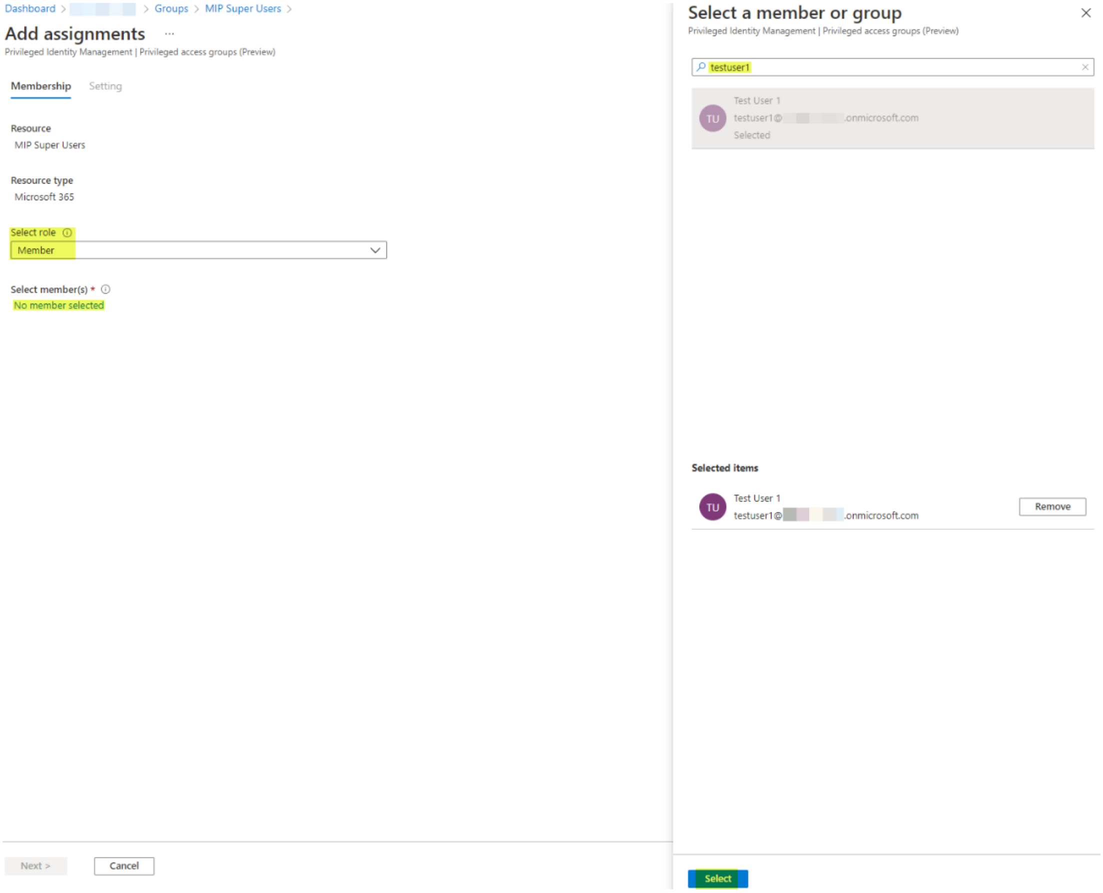


MIP Super Users | Privileged access (Preview) ···

Group

Name	Principal name	Type	Membership	State	Start time	End time
Owner						
[redacted]	[redacted].onmicrosoft.com	User	Direct	Assigned	-	Permanent

10. Under ‘Select role’ choose ‘Member’ and then click the ‘No member selected’ link to add appropriate user accounts that will be eligible for this role:



Dashboard > [redacted] > Groups > MIP Super Users >

Add assignments ...

Privileged Identity Management | Privileged access groups (Preview)

Membership Setting

Resource
MIP Super Users

Resource type
Microsoft 365

Select role ⓘ
Member

Select member(s) * ⓘ
No member selected

Next > Cancel

Select a member or group ×

Privileged Identity Management | Privileged access groups (Preview)

testuser1

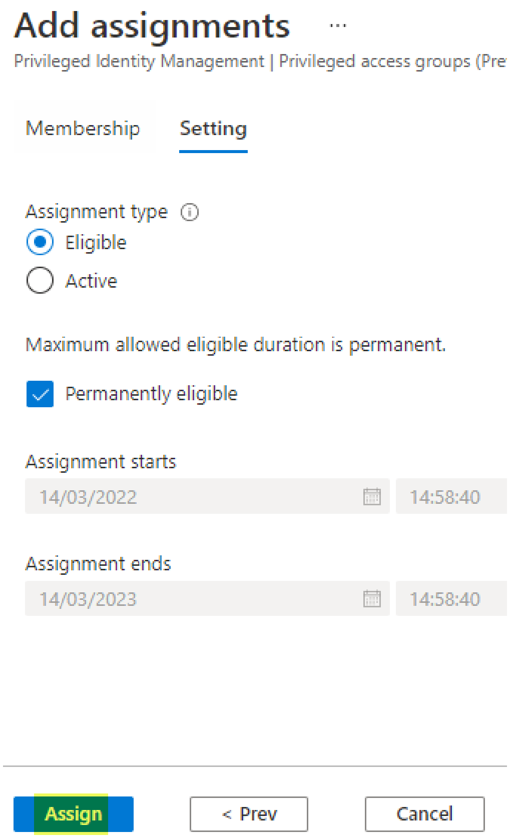
Test User 1
testuser1@[redacted].onmicrosoft.com
Selected

Selected items

Test User 1
testuser1@[redacted].onmicrosoft.com Remove

Select

11. Repeat step 6 for all user accounts that need to be made eligible for this role.
12. Then click ‘Next’
13. Then click ‘Assign’:



Add assignments ...

Privileged Identity Management | Privileged access groups (Pre

Assignment type ⓘ

● Eligible

○ Active

Maximum allowed eligible duration is permanent.

☑ Permanently eligible

Assignment starts

14/03/2022 14:58:40

Assignment ends

14/03/2023 14:58:40

14. Next, on a Privileged Access Workstation with access to your tenant, run the following PowerShell commands:

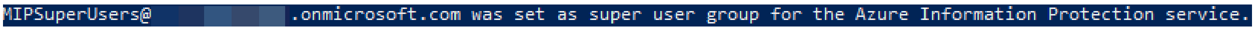
```
Install-Module -Name AIPService -Scope CurrentUser -Force
Connect-AipService
```

Then authenticate using an account that has administrative privileges for Information Protection

```
Enable-AipServiceSuperUserFeature
Set-AipServiceSuperUserGroup -GroupEmailAddress "MPIPSuperUsers@YourTenantHere"
```

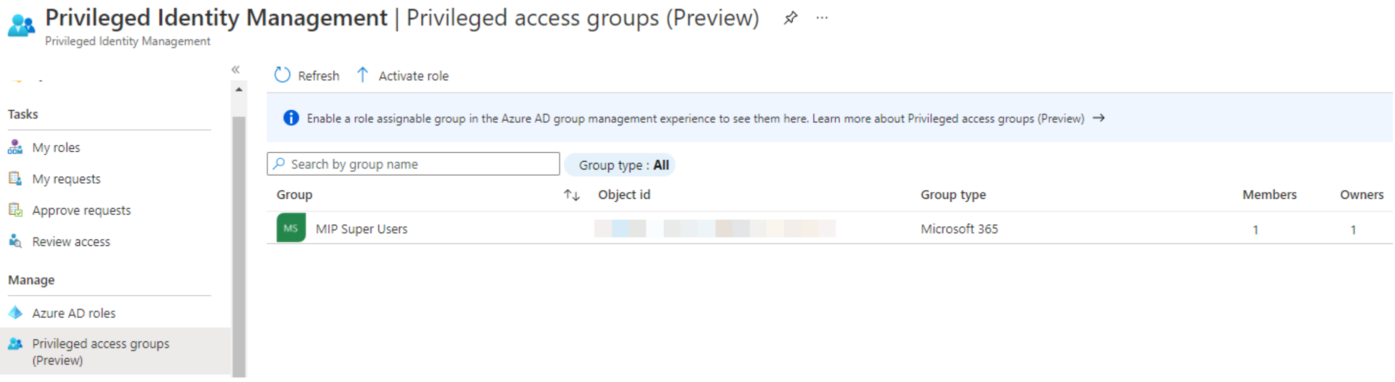
Replace YourTenantHere with the domain name of your tenant.

Once the command has run successfully, you should see the following response:



```
MIPSuperUsers@[redacted].onmicrosoft.com was set as super user group for the Azure Information Protection service.
```

15. For users that want to elevate into this role, have them navigate to [Privileged Identity Management | Privileged access groups (Preview)]:



Privileged Identity Management | Privileged access groups (Preview)

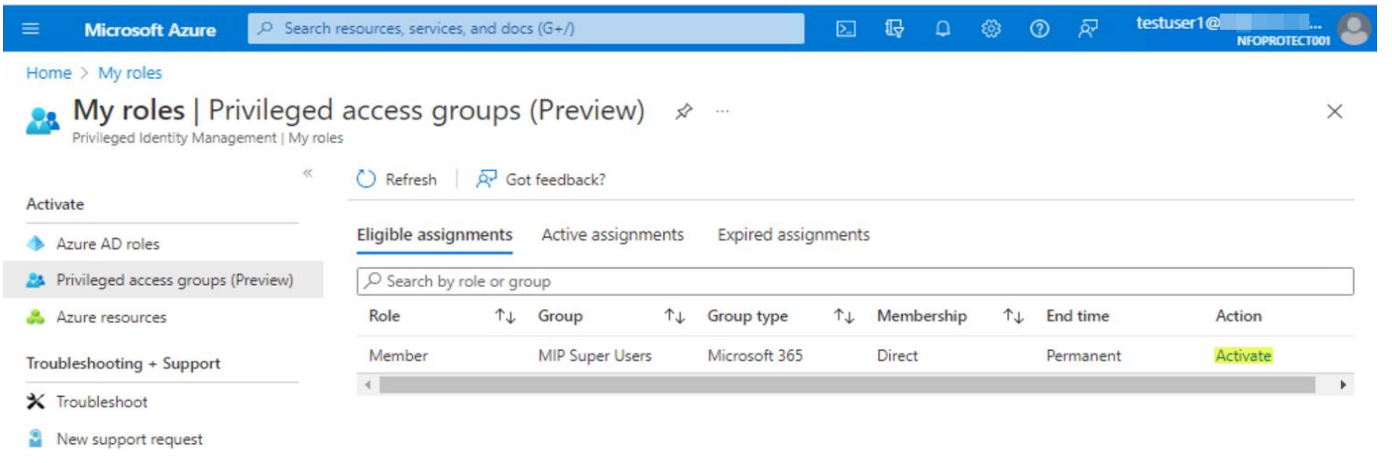
Privileged Identity Management

ⓘ Enable a role assignable group in the Azure AD group management experience to see them here. Learn more about Privileged access groups (Preview) →

Search by group name | Group type : All

Group	Object id	Group type	Members	Owners
MS MIP Super Users	[redacted]	Microsoft 365	1	1

16. Select the super users group from the list, then under ‘My roles’ eligible users will see the role to select in the list. Clicking the ‘Activate’ link will allow them to complete the PIM approval workflow and gain the role (until it expires or they deactivate the role manually):

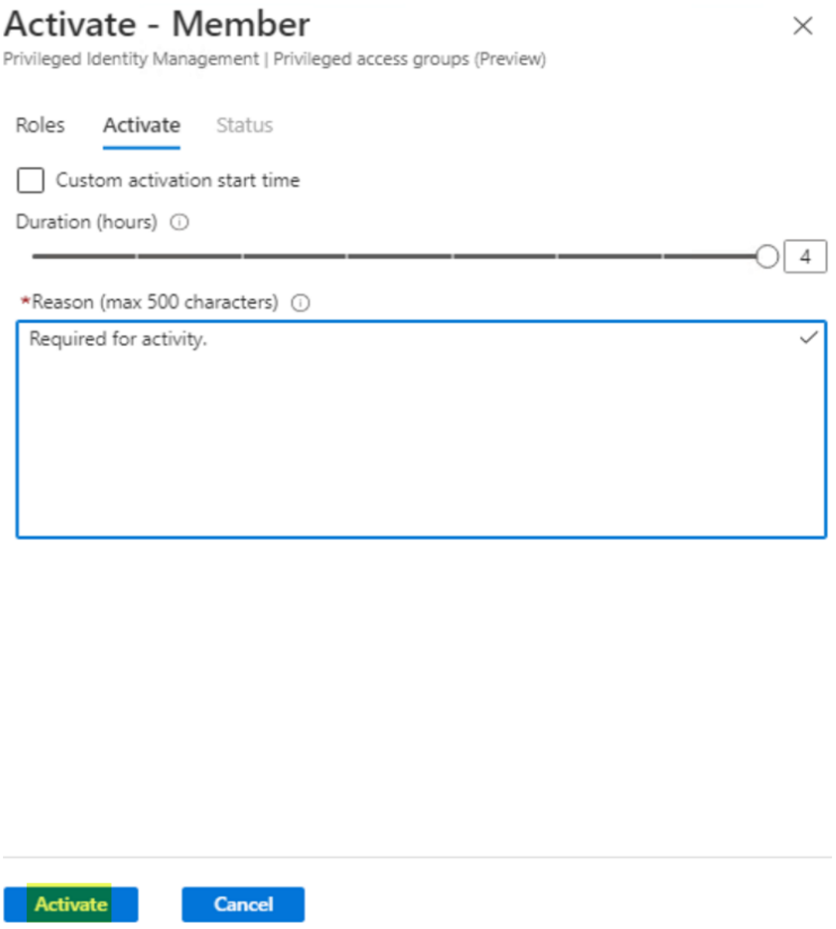


My roles | Privileged access groups (Preview)

Privileged Identity Management | My roles

Role	Group	Group type	Membership	End time	Action
Member	MIP Super Users	Microsoft 365	Direct	Permanent	Activate

17. Provide a suitable justification and click ‘Activate’:



Activate - Member

Privileged Identity Management | Privileged access groups (Preview)

□ Custom activation start time

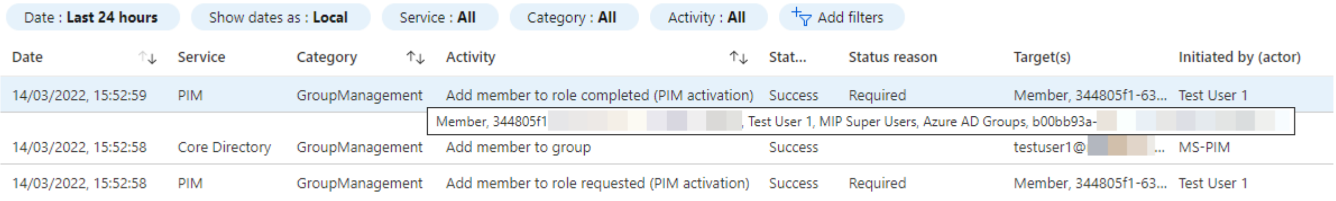
Duration (hours): 4

*Reason (max 500 characters): Required for activity.

18. The user can then perform whatever duties require this role.

Important

Azure AD administrators can verify who is activating this eligible role by viewing the Azure AD | Audit Logs in the Azure portal:



Date	Service	Category	Activity	Stat...	Status reason	Target(s)	Initiated by (actor)
14/03/2022, 15:52:59	PIM	GroupManagement	Add member to role completed (PIM activation)	Success	Required	Member, 344805f1-63...	Test User 1
14/03/2022, 15:52:58	Core Directory	GroupManagement	Add member to group	Success		testuser1@[redacted]...	MS-PIM
14/03/2022, 15:52:58	PIM	GroupManagement	Add member to role requested (PIM activation)	Success	Required	Member, 344805f1-63...	Test User 1

Member, 344805f1[redacted], Test User 1, MIP Super Users, Azure AD Groups, b00bb93a-[redacted]