Dave Campbell
Lead Microsoft 365 Consultant

Get It Sorted!

Information Protection

CompanyNet
company-net.com

CompanyNet

company-net.com

Agenda

Data lifecycle & the vision

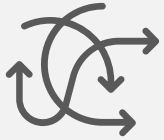
Microsoft Cloud Tools

Sensitivity

Retention

Data Loss Prevention

Data lifecycle governance is vital



Prevent Data Loss

Encryption

Restrict Access

Watermark

Retention

Archiving

CompanyNet

The Vision

Our important information is **protected**

Can’t be accidently or maliciously deleted or lost

Can’t be accidently or maliciously leaked

Sensitive information is marked so it can be protected

We are **compliant**

We retain information we are required to keep

We dispose of information we are not allowed to keep.

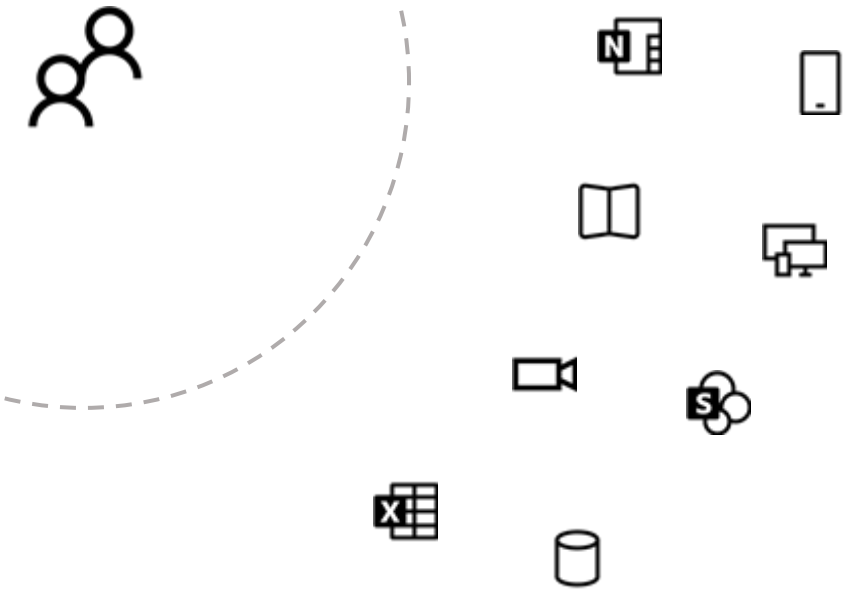
We are **efficient**

Keeping huge amounts of Redundant, Obsolete and Trivial (ROT) information costs – in terms of storage, management, compliance, search & discovery.

CompanyNet

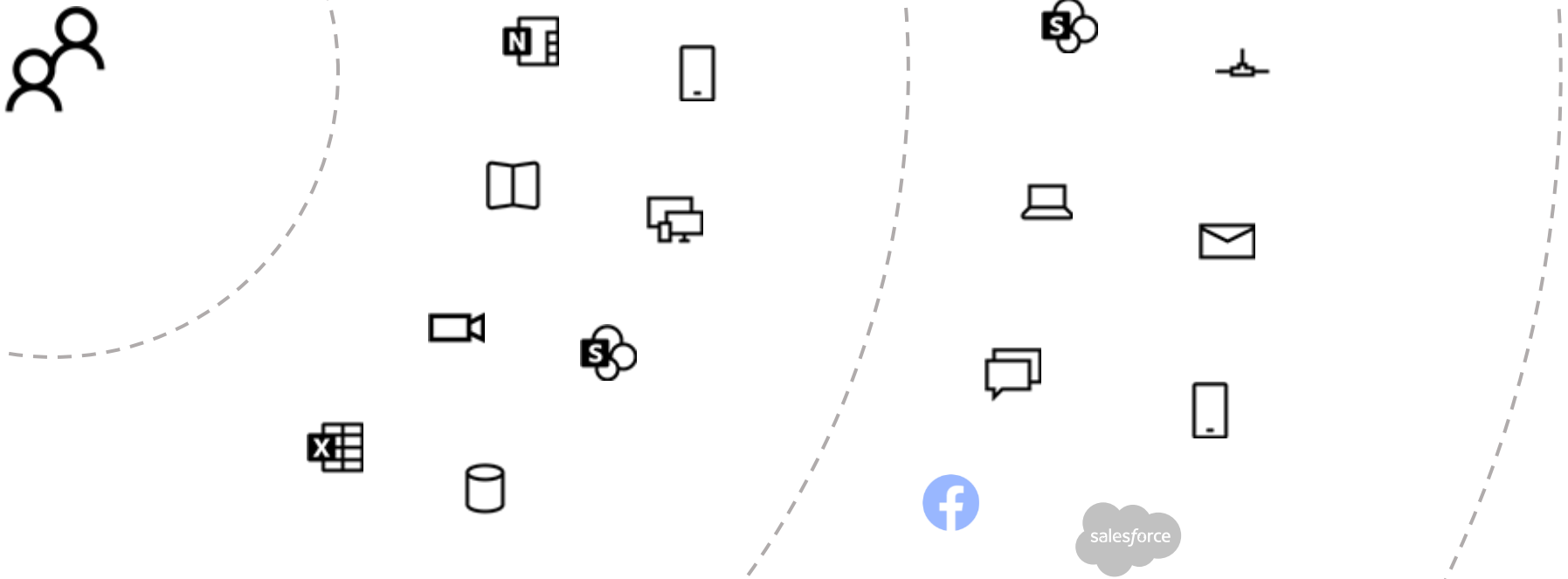
The Data Lifecycle

Data is created



Data is created

Data moves

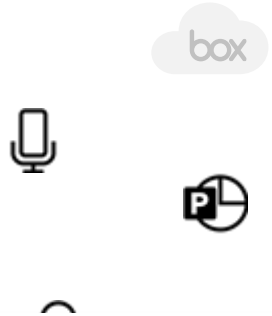


Data is created

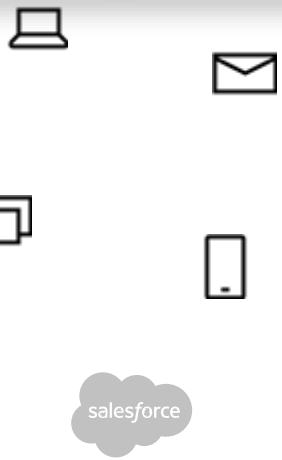
Data moves

Data leaves your company

Know your Data



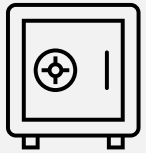
Protect & Govern your Data



Prevent Data loss

The **Microsoft Cloud** introduces powerful tools to aid the vision

Sensitivity



Retention

Data Loss Prevention

CompanyNet

Why?

- Users need to collaborate with others both internally and externally.
- Collaboration technology has made it easier to share information
- Not all information should be shared.

What?

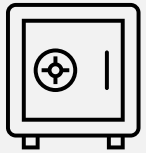
- **Sensitivity Labels** help protect files and emails by:
  - Adding watermarks, headers or footers so that users are aware of the need to protect the information.
  - Encrypting Content
  - Monitoring
- **Sensitivity Labels** can be applied to Teams, Microsoft 365 Groups and SharePoint sites to enforce privacy, external access and unmanaged device access

Sensitivity

CompanyNet

The **Microsoft Cloud** introduces powerful tools to aid the vision

Sensitivity



Retention

Data Loss Prevention

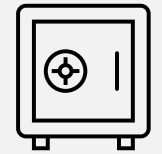
CompanyNet

Why?

- **Comply proactively with industry regulations and internal policies** that require you to retain content for a minimum period of time
- **Reduce your risk in the event of litigation or a security breach** by permanently deleting old content that you're no longer required to keep
- **Help your organization to share knowledge effectively and be more agile** by ensuring that your users work only with content that's current and relevant to them

What?

- A retention policy and or label can help you achieve all of these goals. Managing content commonly requires two actions:
  - **Retaining** content so that it can't be permanently deleted before the end of the retention period
  - **Deleting** content permanently at the end of the retention period

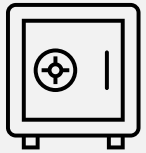


Retention

CompanyNet

The **Microsoft Cloud** introduces powerful tools to aid the vision

Sensitivity



Retention

Data Loss Prevention

CompanyNet

Why?

- Effective collaboration with partners, supply chain, consultants, etc now goes far beyond email:
  - Teams chat and collaboration, SharePoint & OneDrive sharing
- It can be too easy to accidentally or maliciously share sensitive information

What?

- **Data Loss Prevention polices** are used to identify, monitor and protect sensitive information across Office 365.
- **Actions** can notify/warn users or block sharing

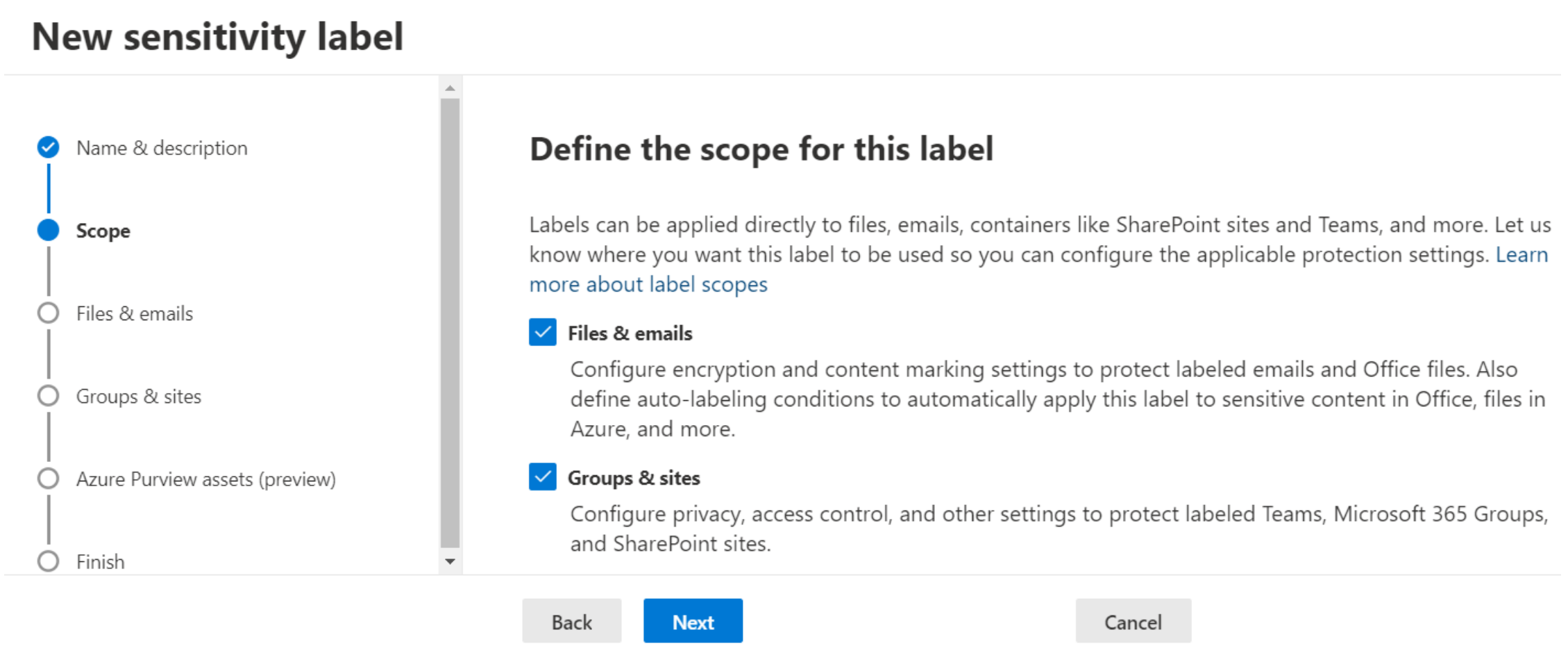
Data Loss Prevention

CompanyNet

Let’s delve deeper into **Sensitivity Labels**

CompanyNet

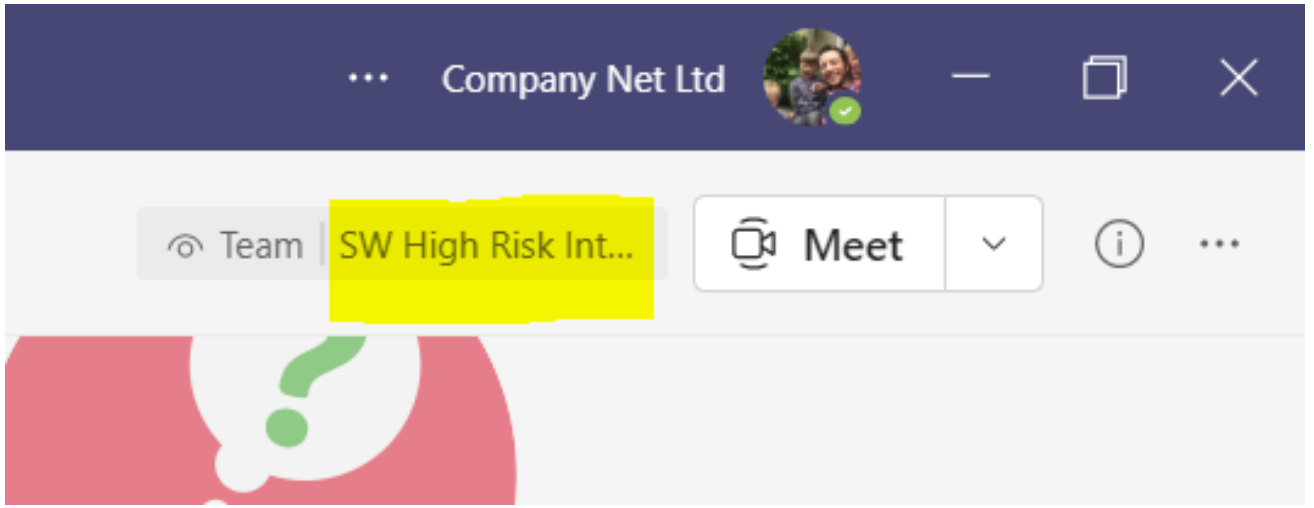
Label Policies



CompanyNet

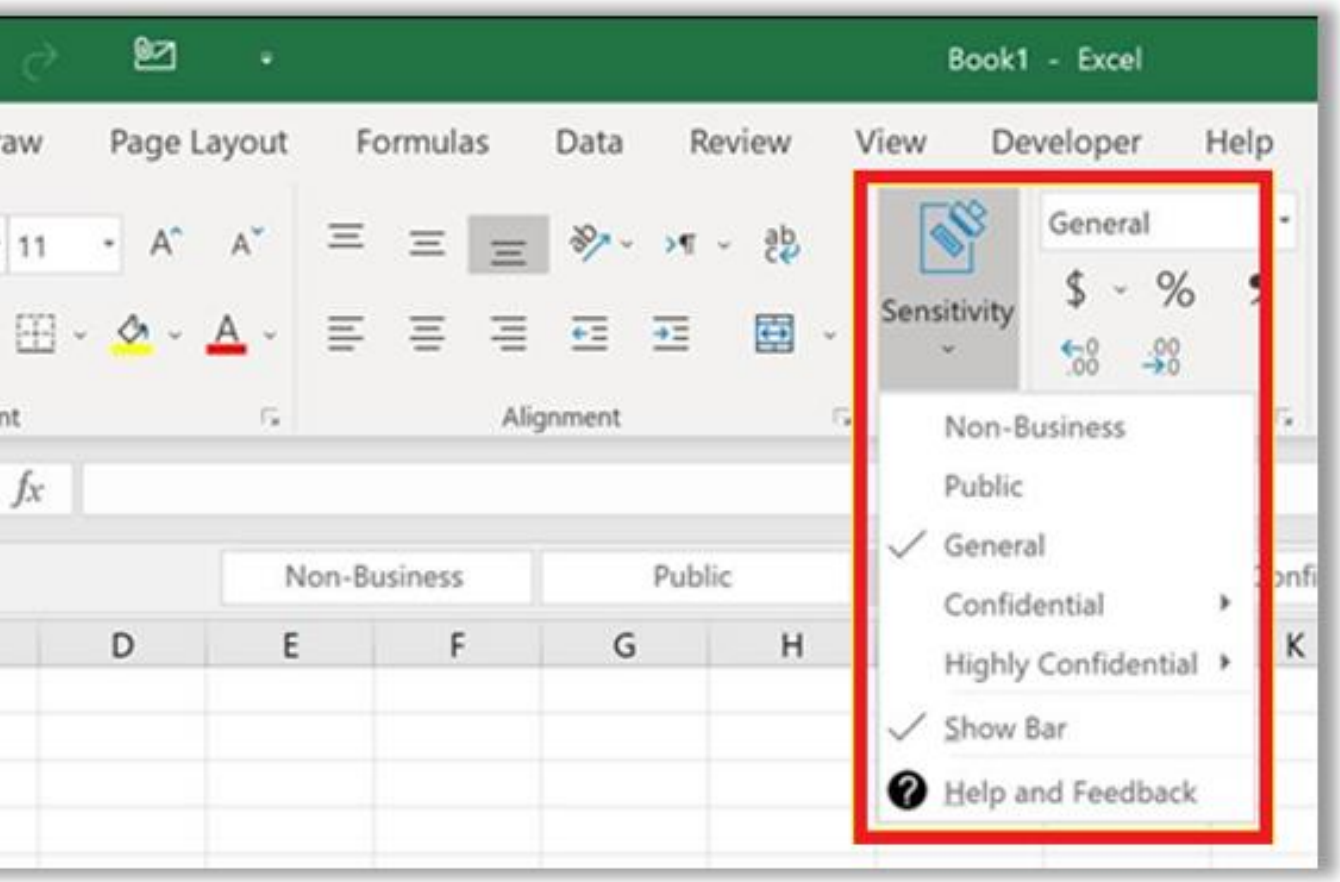
Team, Group and Site Labels (Containers)

- Does **not** label files within containers
- Can enforce:
  - Privacy (public or private) of Teams sites and M365 Groups
  - External user access
  - External sharing from SharePoint sites
  - Access from Unmanaged devices



CompanyNet

Office 365 Sensitivity Labels (Native)

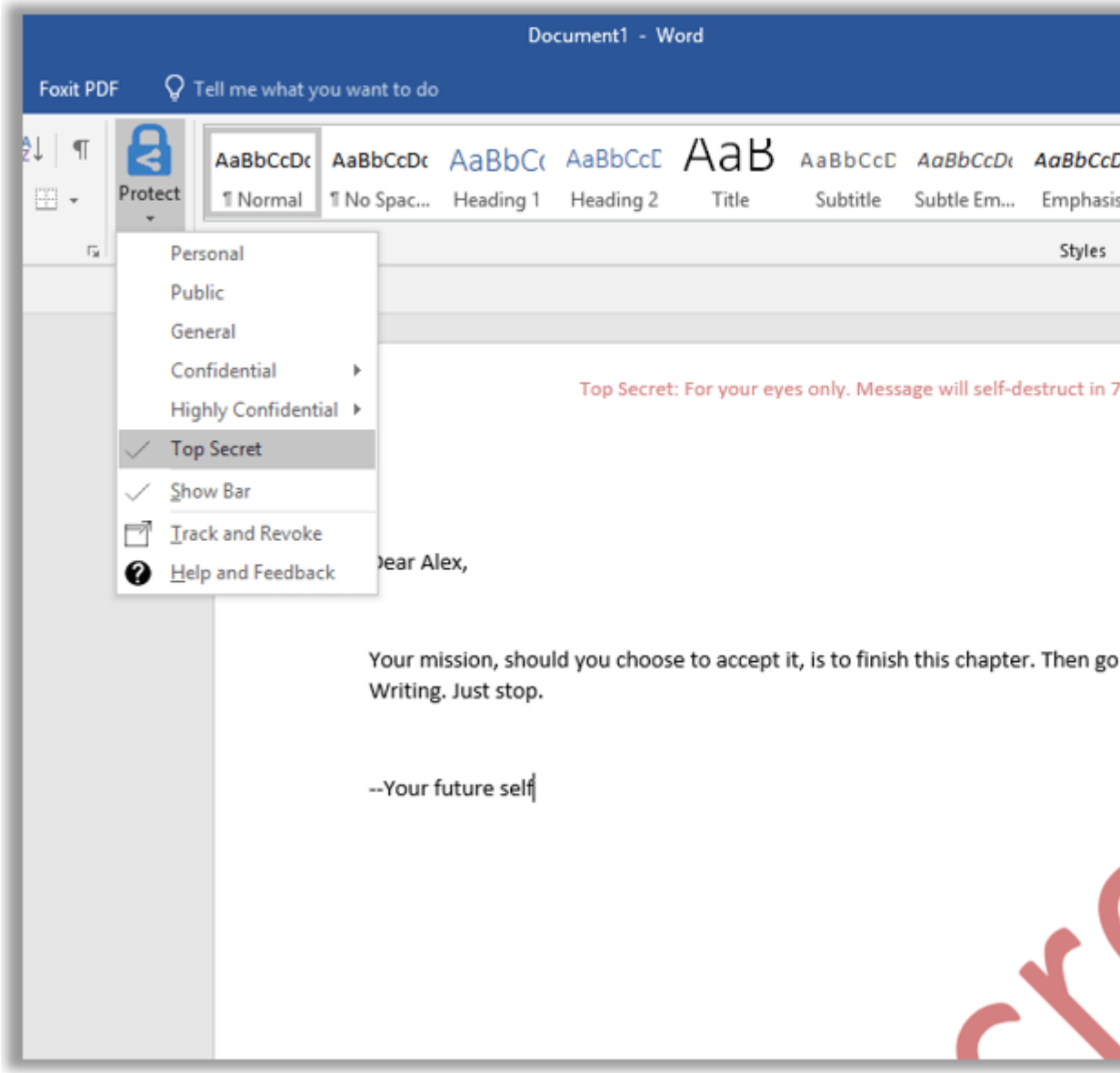


- Used to classify Office documents & emails.
- The label travels with the document.
- Can be used to encrypt a document or email.
- Can be used to add a watermark, header or footer.
- Requires subscription version of office.

CompanyNet

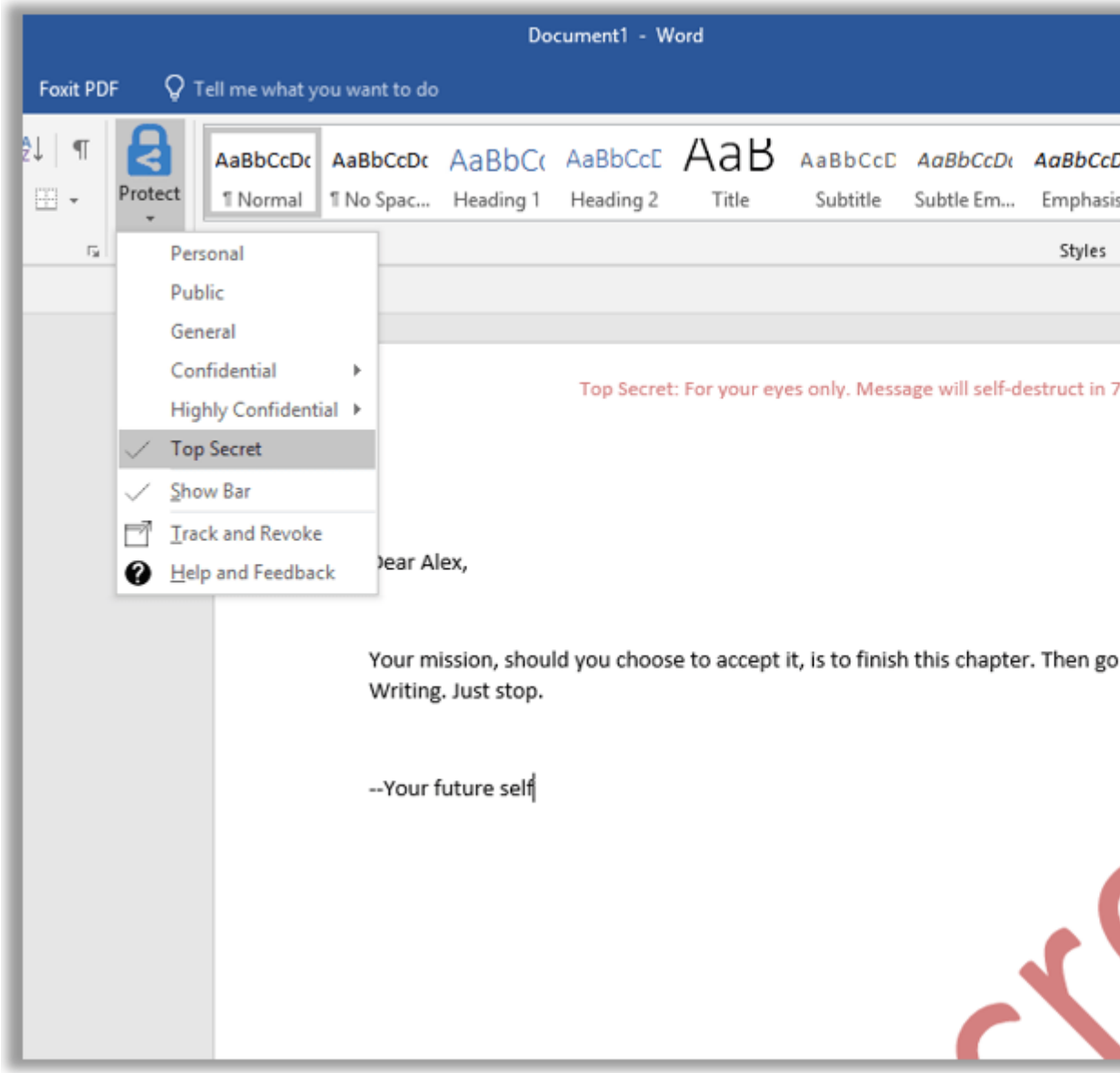
Azure Information Protection (Unified Labeling Client)

- Older and more feature rich than Office 365 Sensitivity Labels.
- Can be used for files outside Office 365 such as those in file shares.
- The UL client allows users to set label in Office applications and by right-clicking files in Explorer.
- The UL client is better suited for hybrid environments.
- An AIP scanner tool can be used on file share to search for and label likely sensitive data like PII



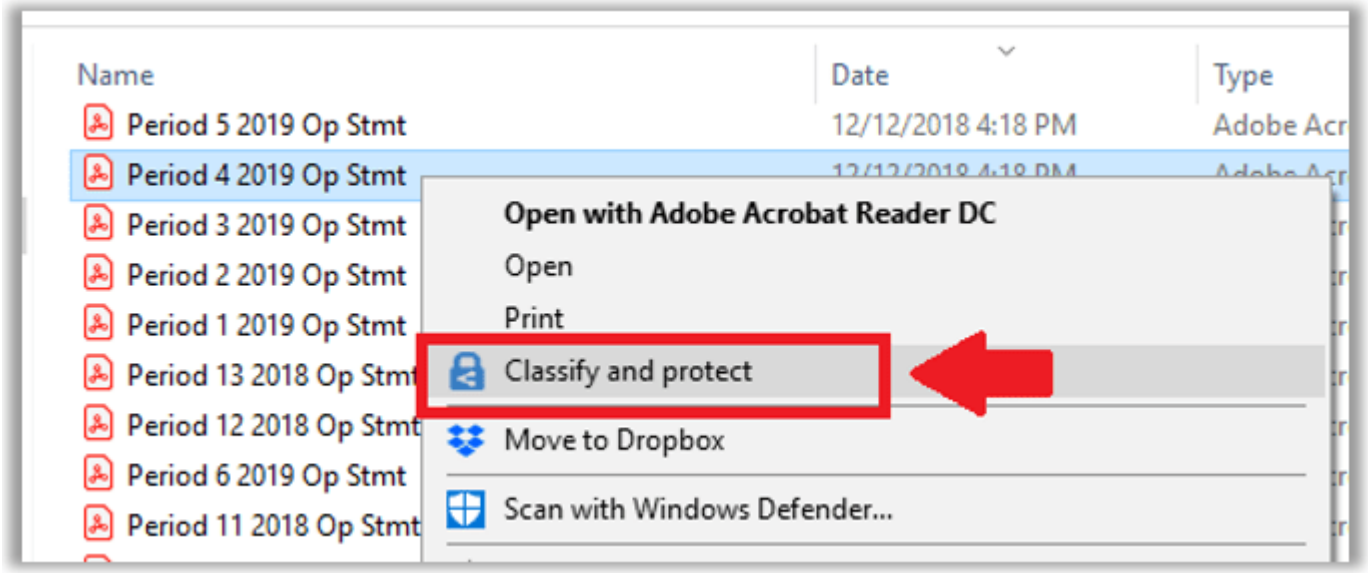
Azure Information Protection Unified Client

- AIP and Office 365 Sensitivity labels can now be sync'd.
- They can then be administered from either Azure or Office 365.
- An updated AIP client has been released that supports both label types.
- It also changes the "Protect" button to "Sensitivity" in Office to align.
- The new Unified client will be further developed.
- The old AIP client will not.



AIP Labels Vs Office 365 Sensitivity Labels

The main difference to note is that AIP is better suited to hybrid environments. You can use the AIP client to encrypt a wider range of file types and those on a traditional file server, for example, right in Windows Explorer.



CompanyNet

Licensing & Features

Feature	Office 365 E5	Office 365 E3	EMS E3
Microsoft Information Protection			
Protect Your Data			
Manage sensitivity labels in Microsoft 365 Apps (Office 365 ProPlus/Business client apps)	●	●	●[6]
Automatically apply sensitivity labels in Microsoft 365 Apps (Office 365 ProPlus/Business client apps) based on sensitive information types	●		
Manually apply sensitivity labels in Office for the Web and Office Mobile	●	●	
Automatically apply sensitivity labels in Office for the Web and Office Mobile based on sensitive information types	●		
Manually apply sensitivity labels to SharePoint sites, Teams, and Microsoft 365 Groups	●[7]	●[7]	
Automatically apply sensitivity labels to data in Office perpetual and SharePoint Server on-premises using AIP client (incl. AIP scanner)			
Automatically apply sensitivity labels to files in SPO or to EXO email	●		
Manually apply sensitivity labels to data in 3rd party clouds			●[9]
Automatically apply sensitivity labels to data in 3rd party clouds			
Apply and view sensitivity labels in Power BI, and protect data when it is exported to Excel, PowerPoint or PDF	●[7]		●[8]
Auto-labeling policy simulation	●		
Enable 3rd party integration into Microsoft Information Protection (MIP) using MIP SDK			●
Basic Office 365 Message Encryption	●	●	●
Advanced Office 365 Message Encryption	●		
Customer Key for Office 365	●		
Double Key Encryption	●		
Bring Your Own Key (BYOK) for customer-managed key provisioning life cycle[13]			●

CompanyNet

Let’s delve deeper into **Retention**

CompanyNet

Retention in Office 365

- There are two ways that you can retain and delete information in Office 365:
  - **Retention labels** manage retention and deletion. They can do disposition reviews, event-based retention, and more. However, you can only use them to manage SharePoint, OneDrive, Office 365 Groups, and Exchange email content.
  - **Retention Policies** also allow you to manage content for retention deletion. They're broad policies that you can use to manage Microsoft Teams, Skype for business, Exchange, SharePoint, OneDrive, Exchange public folder content. They can also manage the content sources listed under retention labels.
- These are designed to work together.

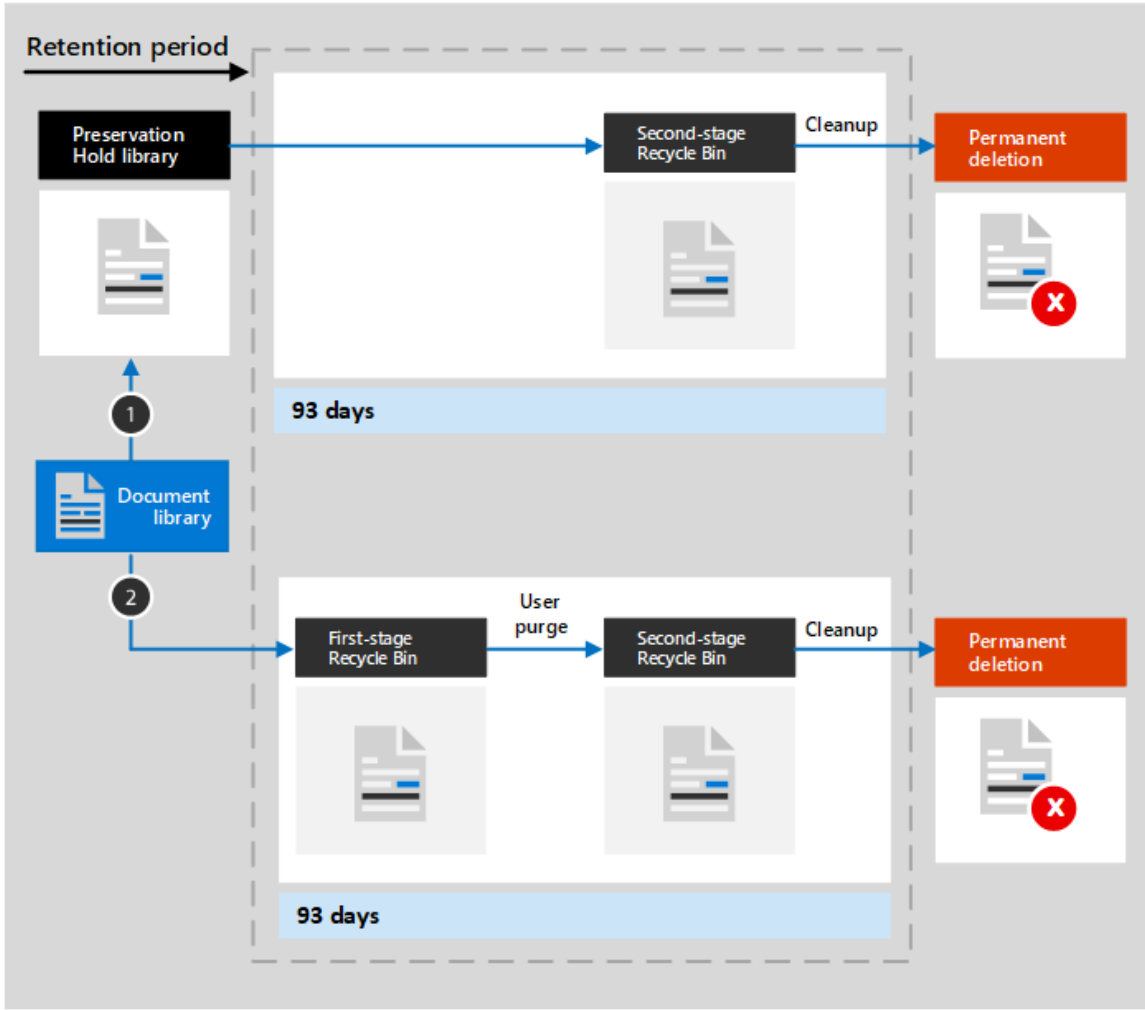
CompanyNet

	Retention Policy	Retention Label
Applied by	Admin	User
Applied to	Site collection, mailbox, OneDrive account	Document, email, folder, document library
Retention	X	X
Deletion	X	X
Disposition Review		X
Retain or delete based on…	Created, Modified	Created, Modified, When Labelled, Event
Can be applied to…	Exchange SharePoint OneDrive Office 365 Group Skype for Business Exchange Public Folders Microsoft Teams	Exchange SharePoint OneDrive Office 365 Groups

How does Retention work?

When content is subject to a retention policy, people can continue to edit and work with the content as if nothing has changed because the content is retained in place, in its original location. But if someone edits or deletes content that is subject to the policy, a copy is saved to a secure location where it is retained while the policy is in effect.

SharePoint and OneDrive



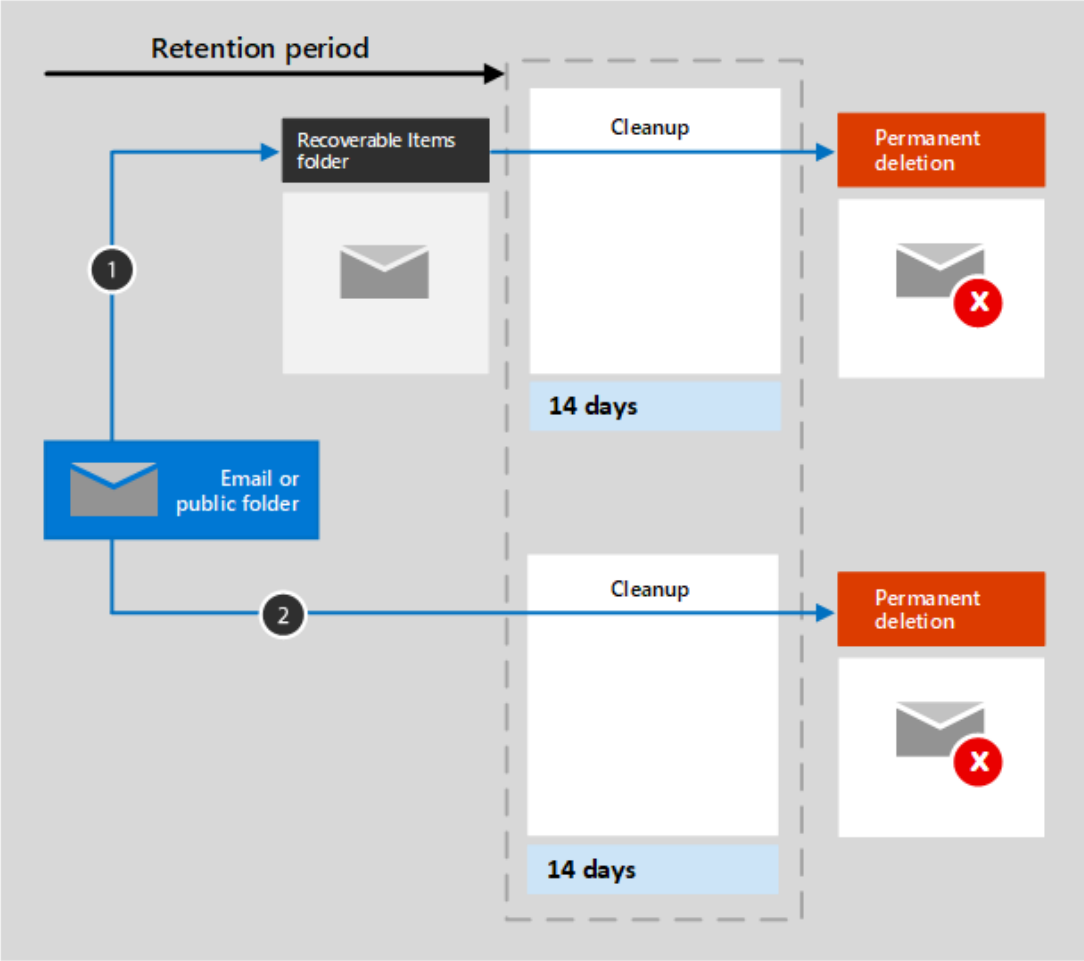
1. **If the content is modified or deleted**
2. **If the content is not modified or deleted**

CompanyNet

How does Retention work?

For a user's mail, calendar, and other items, a retention policy is applied at the level of a mailbox. For a public folder, a retention policy is applied at the folder level, not the mailbox level. Both a mailbox and a public folder use the Recoverable Items folder to retain items. Only people whom have been assigned eDiscovery permissions can view items in another user's Recoverable Items folder.

Mailboxes and Public Folders



1. **If the content is modified or deleted**
2. **If the content is not modified or deleted**

CompanyNet

The principles of Retention

CompanyNet

Licensing & Features

Feature	Office 365 E5	Office 365 E3	EMS E3
Microsoft Information Governance			
Retention Policy and Labels			
Manually apply non-record retention labels	●	●	
Apply a default retention label for SharePoint libraries, folders, and document sets	●		
Retention labels disposition review	●		
Automatically apply a retention label to emails by using Outlook rules	●		
Apply a basic retention policy to the entire organization, specific locations or users	●	●	
Automatically apply retention policies based on specific conditions (e.g., keywords or sensitive information)	●		
Automatically apply retention policies based on Machine Learning (trainable classifiers)			
Automatically apply retention policies based on an event	●		
Bulk-import PST files to Exchange Online mailboxes	●[10]	●[10]	
3rd-party data connectors	●		
Email archiving	●[10]	●[10]	
Advanced features for inactive mailboxes [16]	●		

CompanyNet

Let’s delve deeper into **Data Loss Prevention**

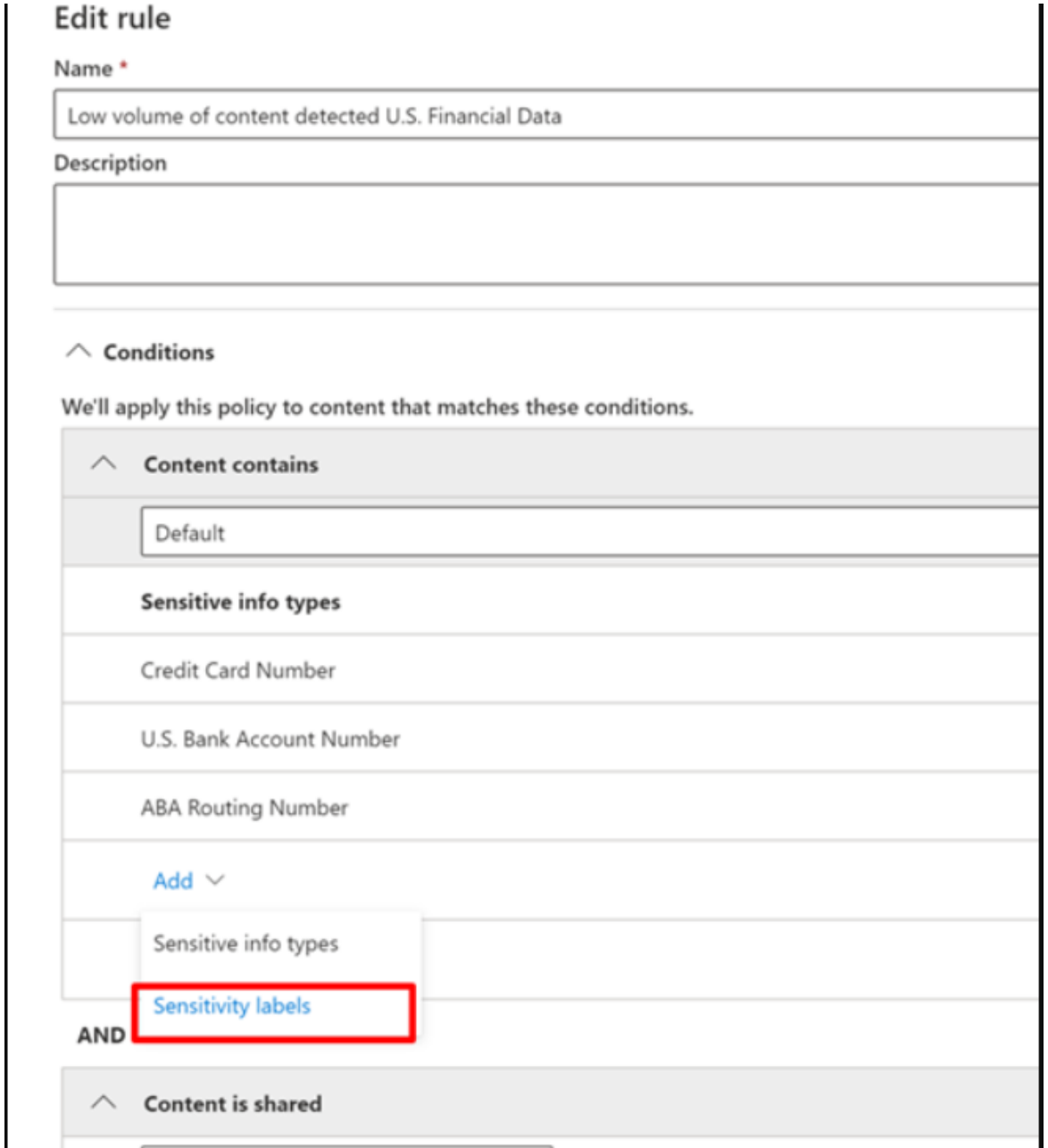
CompanyNet

Data Loss Prevention Policies

- A DLP policy can identify, monitor and protect sensitive items across:
  - Teams, Exchange, SharePoint and OneDrive
  - Office applications
  - Windows 10 devices
- When certain conditions are met, protective actions are taken
  - Show a pop-up policy tip to the user to warn them they may be trying to share a sensitive item inappropriately
  - Block the sharing and allow the user to override and capture the users' justification
  - Block the sharing with/without override option
  - For data a rest, sensitive items can be locked and moved to a secure quarantine locations
  - For Teams chat, the sensitive info will not be displayed

Policy Rules

- Monitor
  - Predefined policy templates: Financial data, Medical data, Privacy data for various countries
  - A custom policy that uses sensitivity info types, retention labels and sensitivity labels
- Locations
  - Exchange, SharePoint, OneDrive
  - Teams chat and channel messages
  - Windows 10 devices
  - MCAS
  - On-premise repositories
- Conditions
  - Item contains sensitive information
  - Item has sensitivity label
  - Item is shared internally or externally



Actions

- Choose the action to take when the policy conditions are met - The actions depend on the location where the activity is happening.
- Some examples are:
  - SharePoint/Exchange/OneDrive: Block people who are outside your organization form accessing the content. Show the user a tip and send them an email notification that they are taking an action that is prohibited by the DLP policy.
  - Teams Chat and Channel: Block sensitive information from being shared in the chat or channel
  - Windows 10 Devices: Audit or restrict copying a sensitive item to a removeable USB device
  - Office Apps: Show a popup notifying the user that they are engaging in a risky behavior and block or block but allow override.

Licensing & Features

Feature	Office 365 E5	Office 365 E3	EMS E3
Microsoft Information Protection			
Data Loss Prevention			
Office 365 DLP for files and email	●	●	
Communication DLP (Teams chat and channel conversations)	●		
Endpoint DLP			

CompanyNet

The **Microsoft Cloud** has many more tools that aid security and compliance across your tenant

Contact us to learn more!
www.company-net.com

CompanyNet