The logo for T-Minus 365 features the text "T-MINUS" in a grey, sans-serif font. A blue curved line starts from the top of the letter "M" and arches over to the right, ending in a small blue arrowhead. To the right of "T-MINUS" is a blue cloud shape containing the white text "365".

T-MINUS 365

**Setting Up M365
Data Loss
Prevention**

Prepared by

Nick Ross

Microsoft Certified Expert Administrator

(msp4msps@tminus365.com)

Guide Description

*The purpose of this guide is to lay out the steps for configuring Azure Information Protection and DLP Policies. This guide is assuming you have the **M365 Business** License but can be applied to the following licenses:*

- *Azure Information Protection Plan 1*
- *EMS +E3, E5*
- *Office 365 E3 and greater*
- *Office 365 G3 and G5*
- *Office 365 A1, A3, and A5*

****Disclaimer****

This guide is meant to provide best practices for policy creation and implementation of labels. It is meant to be used as a template, but the policies defined will not be the same in all use cases. You must access to policies and configuration you will need for your customers environment and make changes as needed. TMINUS is not liable for any policies you create that do not meet the customers standards. As a best practice, test all configurations with a pilot group before moving to broad deployment across an entire organization

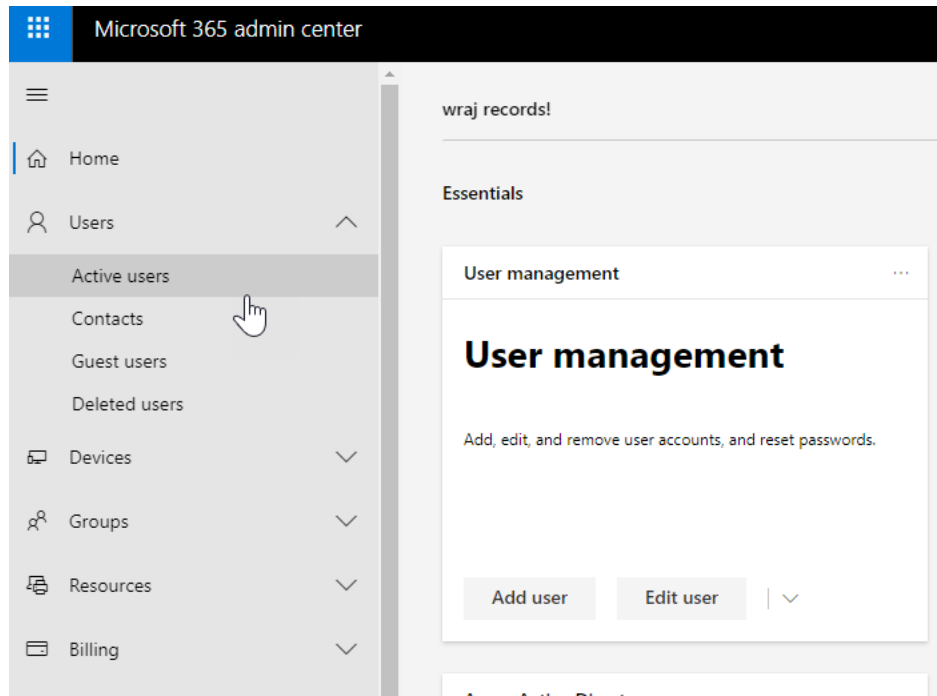
Table of Contents

Table of Contents.....	3
Licensing Users.....	4
Azure Information Protection.....	5
Download the Plugin.....	5
Modifying and Creating Labels	6
Data Loss Prevention Policies	16
Retention Policies	22
Conclusion.....	26

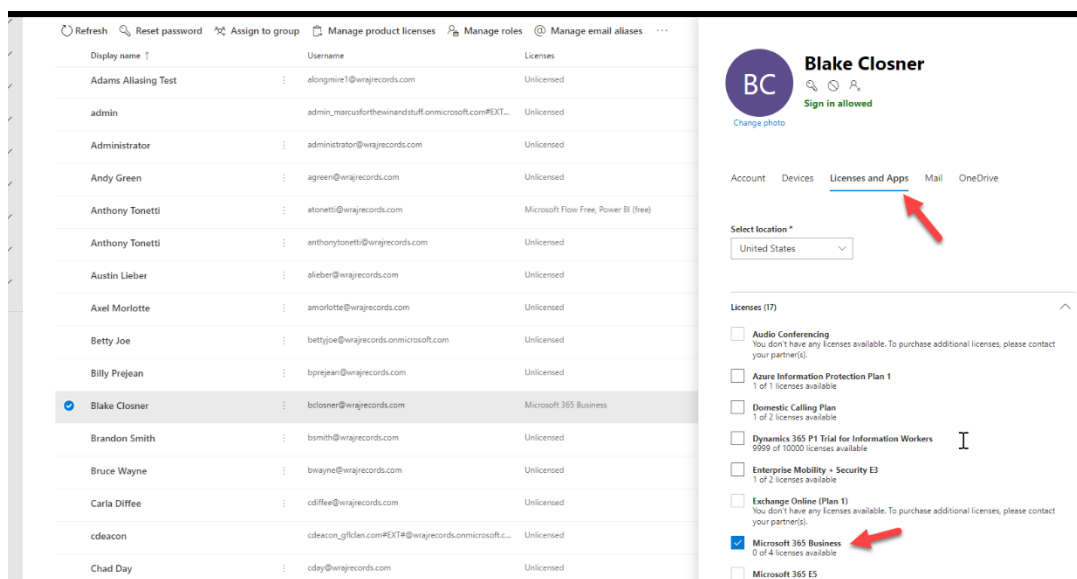
Licensing Users

1. Ensure All appropriate Users are Licensed

a. Login to 365 Admin Center > Go to Active User



b. Select a User > Click **Licenses and Apps** > Ensure an M365 License is Assigned (or license defined on page 1)



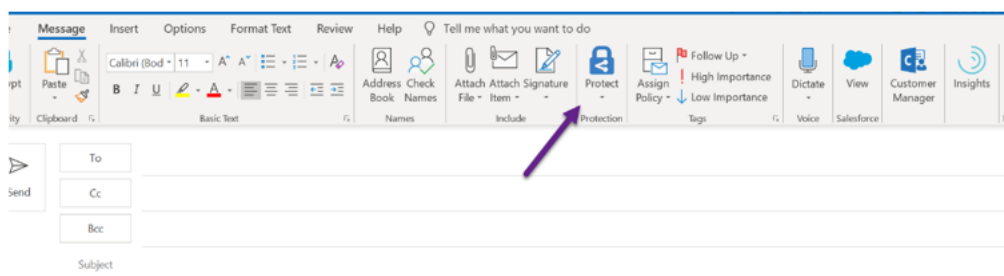
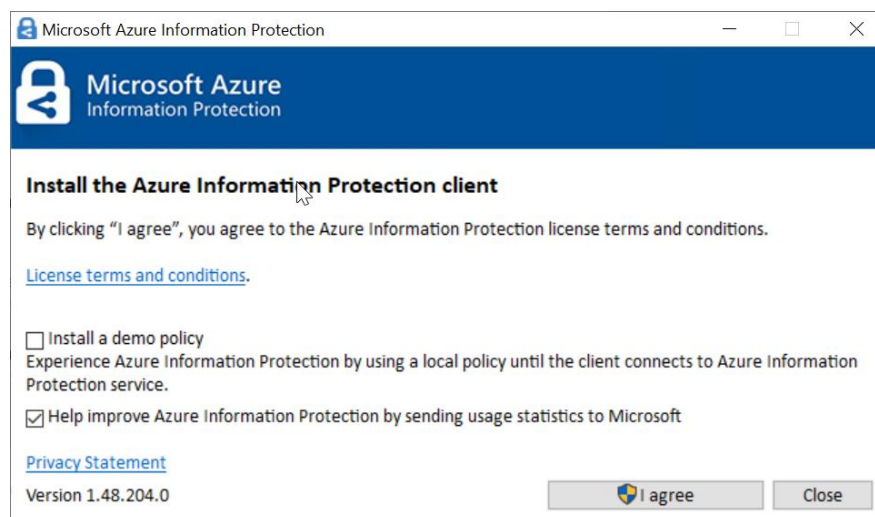
Azure Information Protection

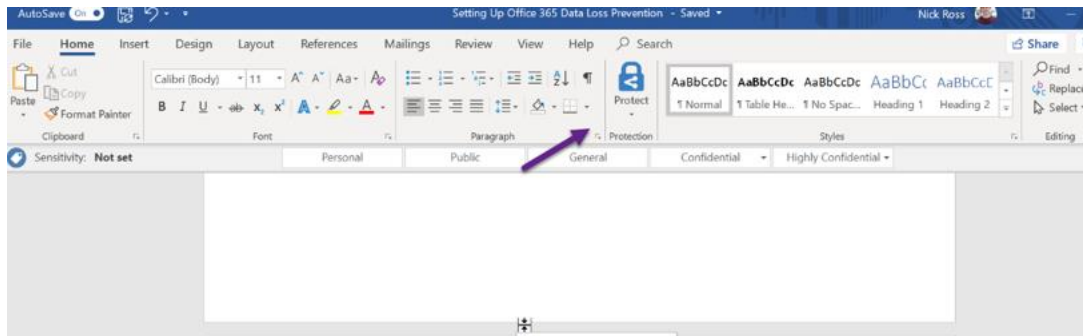
Azure information protection can be used to classify, label, and protect your companies' documents and email. AIP provides the following benefits:

- Secure your files and emails
 - Encryption, identity, authorization policies
- Platform independent
 - Phones, tablets, PCs (iOS/Android)
- Automatically apply policies, classify data, and apply encryption based of keywords or sensitive information (PII, SSN, etc.)

Download the Plugin

- a. You can install a plugin for outlook/office apps that gives users an Azure Information Protection button in their local outlook client and on top of their office suite toolbar. You can create custom labels to apply encryption to messages or documents. Here is [the link for the download](#):

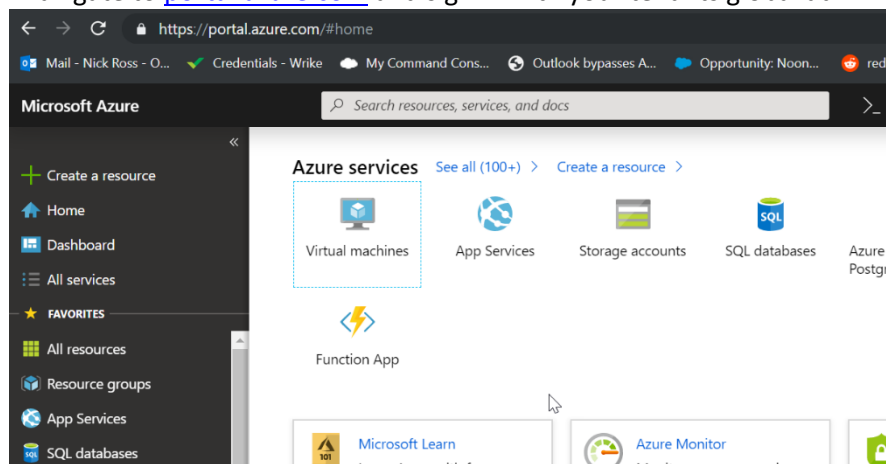




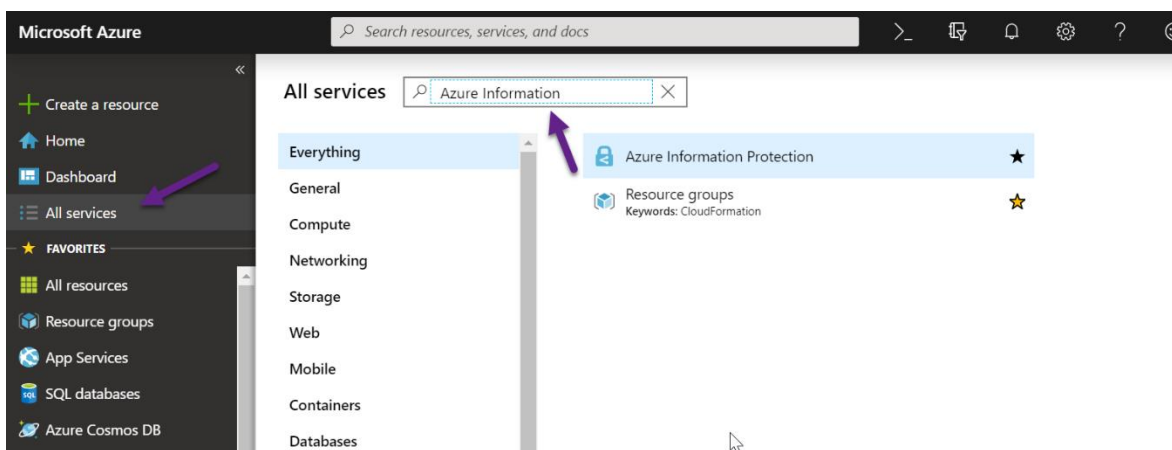
Modifying and Creating Labels

By default, there is a global policy in place with default labels that we can already apply to documents and emails. In this section we are going to look at modifying existing labels and creating a new label of our own:

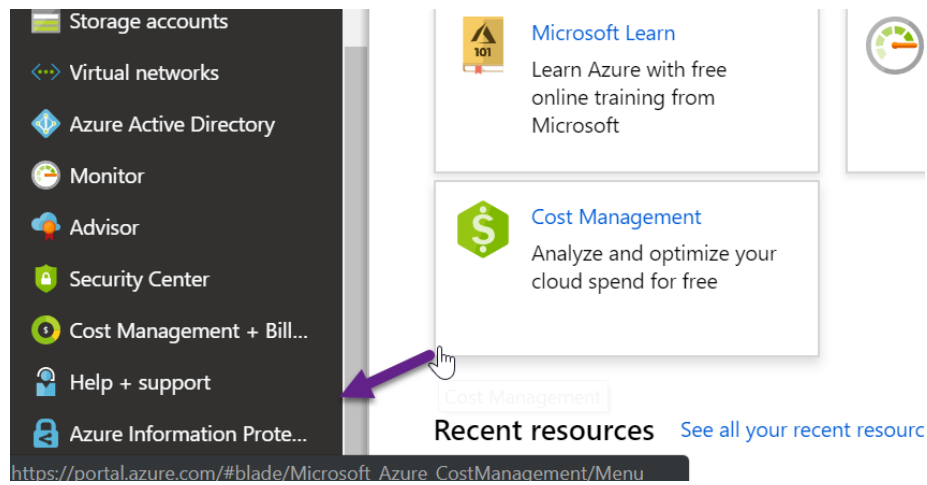
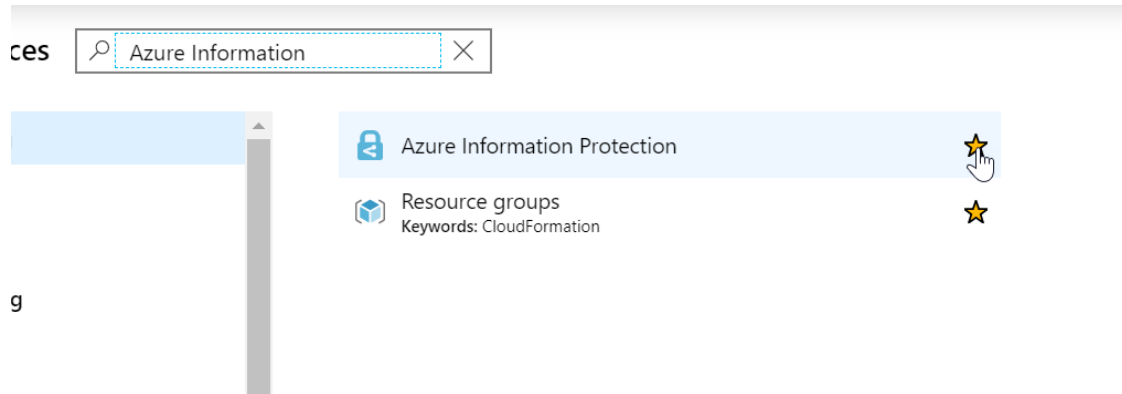
- a. Navigate to portal.azure.com and sign in with your tenants global admin credentials:



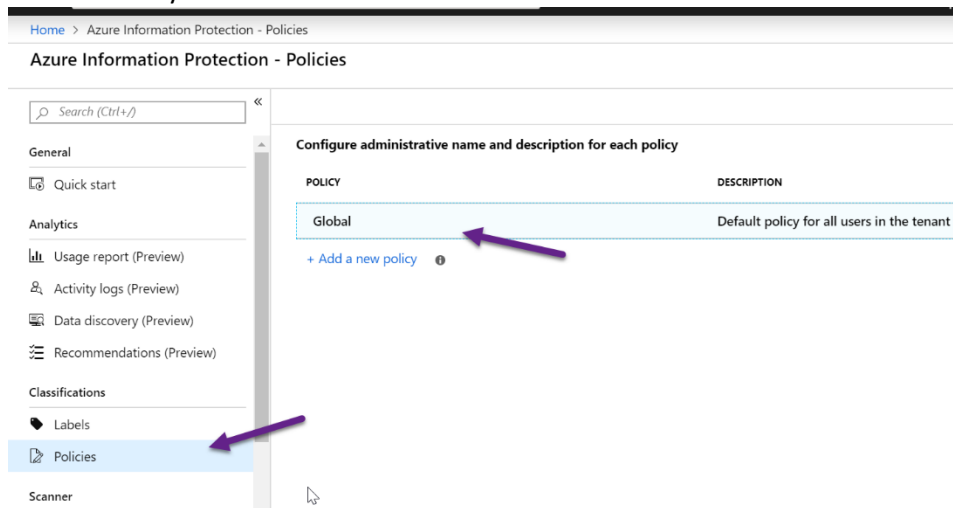
- b. Click on “All Services” and search for Azure Information Protection



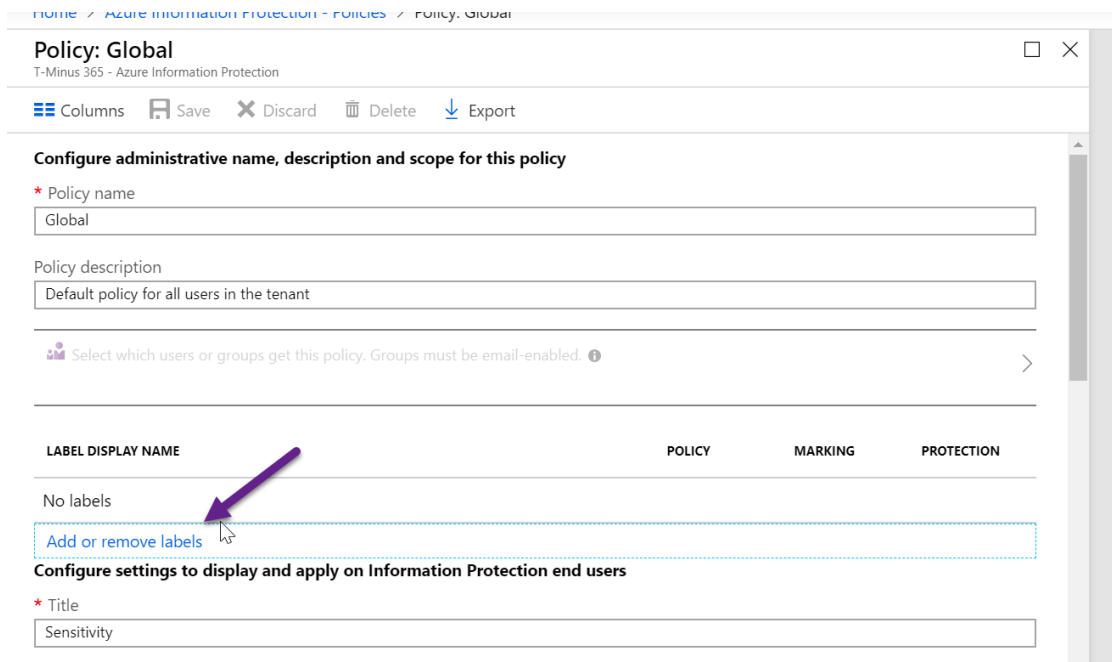
c. Note: You can Star this to Add to your favorite's menu:



d. First, we will look at the default Global Policy by clicking on “Policies” and selecting the “Global Policy”



e. By default, there are no labels assigned to the policy so you will need to do that:



Policy: Global
T-Minus 365 - Azure Information Protection

Columns Save Discard Delete Export

Configure administrative name, description and scope for this policy

* Policy name
Global

Policy description
Default policy for all users in the tenant

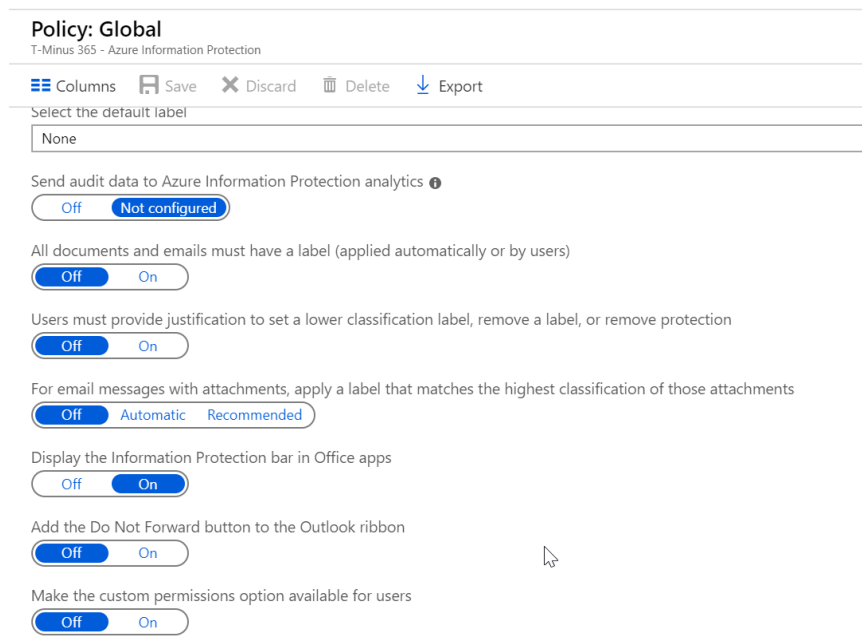
Select which users or groups get this policy. Groups must be email-enabled. >

LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION
No labels			
Add or remove labels			

Configure settings to display and apply on Information Protection end users

* Title
Sensitivity

f. This is the default policy applied to all users. We can see different settings that we can configure. If you wanted to scope policies to certain groups of users, then you can create a new policy. For example, maybe I want to require all of my users in the Finance department to be required to apply a label when saving a document. I can create a new policy specifically for that.



Policy: Global
T-Minus 365 - Azure Information Protection

Columns Save Discard Delete Export

Select the default label
None

Send audit data to Azure Information Protection analytics
Off Not configured

All documents and emails must have a label (applied automatically or by users)
Off On

Users must provide justification to set a lower classification label, remove a label, or remove protection
Off On

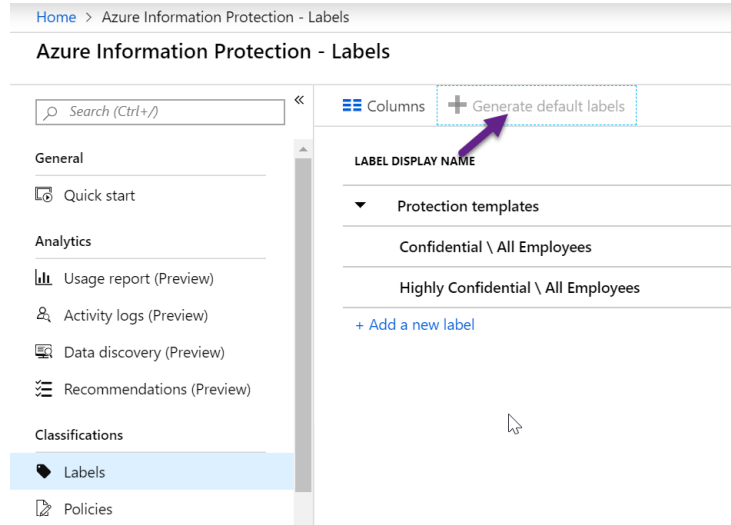
For email messages with attachments, apply a label that matches the highest classification of those attachments
Off Automatic Recommended

Display the Information Protection bar in Office apps
Off On

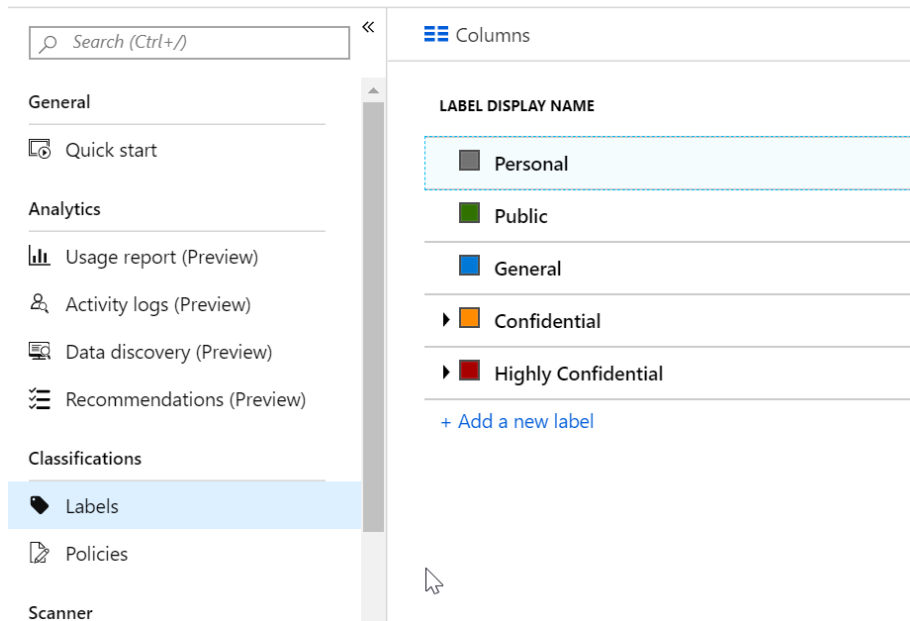
Add the Do Not Forward button to the Outlook ribbon
Off On

Make the custom permissions option available for users
Off On

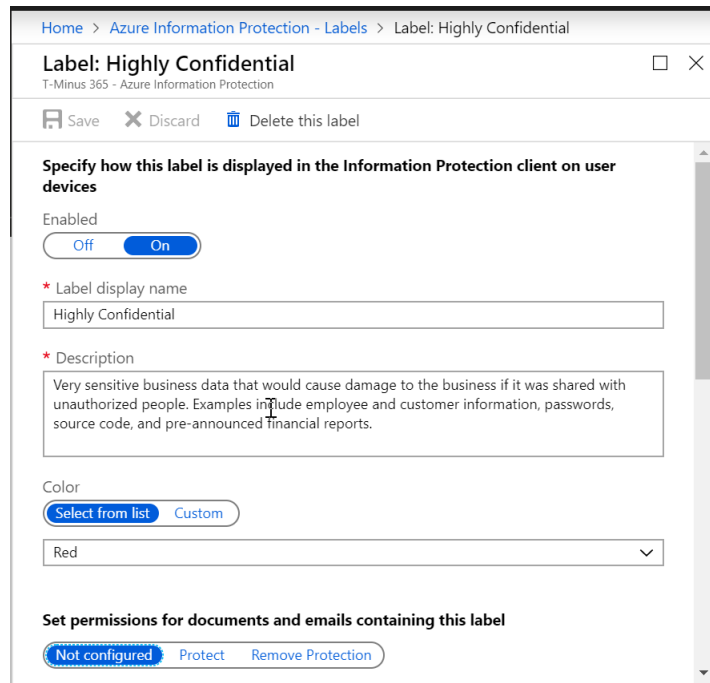
- g. Now we can click “Labels” and take note of the different labels that can already be applied. If you have a newer office 365 tenant, then you may need to click on the “Generate Default labels” to see more:



Azure Information Protection - Labels

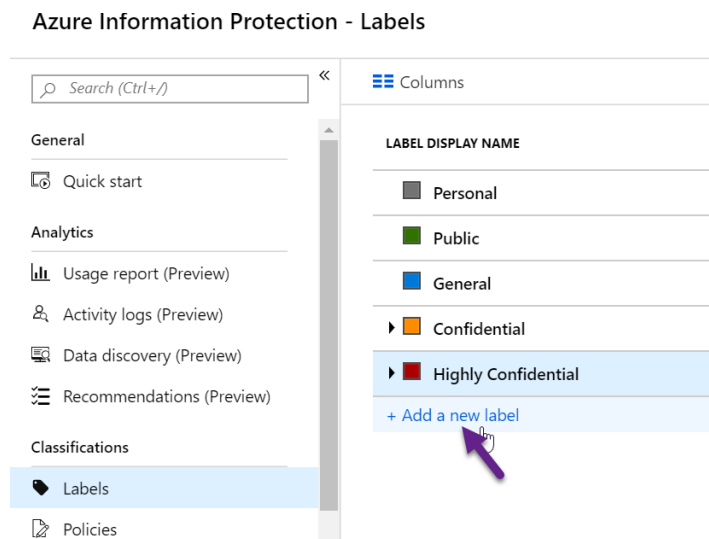


- h. If you click into any label, you will be able to see its settings:



- i. Let's create a label to Encrypt messages/documents outside our organization. From the labels page, click "Add new Label"

Azure Information Protection - Labels



j. Enter your name, description, color:

Dashboard > Azure Information Protection - Labels > Label: Encrypt

Label: Encrypt
wraj records1 - Azure Information Protection

Save Discard Delete this label

Specify how this label is displayed in the Information Protection client on user devices

Enabled
Off On

* Label display name
Encrypt

* Description
encrypt email and Docs ✓

Color
Select from list Custom
Black

k. Click on **Protect**. Here we will be able to granularly define our settings. Leave Set Permissions and click **+Add Permissions** to define your scope of users this will apply to:

Home > Azure Information Protection - Labels > Label > Protection

Label
T-Minus 365 - Azure Information Protection

Save Discard Delete this label

Set permissions for documents and emails containing this label

Not configured Protect Remove Protection

Protection
Azure (cloud key) !

Set visual marking (such as header or footer)

Protection
T-Minus 365 - Azure Information Protection

Protection settings ⓘ

Azure (cloud key) HYOK (AD RMS)

Select the protection action type ⓘ

Set permissions
 Set user-defined permissions (Preview)

USERS **PERMISSIONS**

No permissions are specified

+ Add permissions

File Content Expiration

Never By date By days

- I. Here I can define my scope of users that I want this label to apply to. I am going to select the entire org but I could narrowly define different users/groups/departments if I wanted to and give them certain permissions to the documents. Click ok when complete

Ex. I want to give my HR department Co-Owner rights but everyone else in the org should have viewer rights.

Add permissions


T-Minus 365 - Azure Information Protection

Specify users and groups

Select from the list

[Enter details](#)

- [+ Add T-Minus 365 - All members](#) ⓘ
- [+ Add any authenticated users](#) ⓘ
- [+ Browse directory](#)

USERS 


No users or group specified

Add permissions

T-Minus 365 - Azure Information Protection

Choose permissions from preset or set custom ⓘ

Co-Owner
Co-Author
Reviewer
Viewer
Custom

PERMISSIONS 

<input checked="" type="checkbox"/> View, Open, Read (VIEW)
<input checked="" type="checkbox"/> View Rights (VIEWRIGHTSDATA)
<input checked="" type="checkbox"/> Edit Content, Edit (DOCEDIT)
<input checked="" type="checkbox"/> Save (EDIT)
<input checked="" type="checkbox"/> Print (PRINT)
<input checked="" type="checkbox"/> Copy (EXTRACT)
<input checked="" type="checkbox"/> Reply (REPLY) **
<input checked="" type="checkbox"/> Reply All (REPLY ALL) **

- m. I can also define if I want the document only to be viewed for a limited period of time and if I want to allow offline access. An example would be monthly reports sent out to the finance department that you want to expire after a specified time frame. I will leave these defaulted in this example.

File Content Expiration

Never
 By date
 By days

Allow offline access

Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. [More information and recommended settings](#)

Always
 Never
 By days

Number of days the content is available without an Internet connection

Protection template ID - template id is automatically generated after template is saved

OK

- n. You can configure additional settings here such as header/footer messages and adding watermarks. To configure conditions for auto-applying a label, you **need at least Azure Information Plan 2 subscription**

Set visual marking (such as header or footer)

Documents with this label have a header

Off On

Documents with this label have a footer

Off On

Documents with this label have a watermark

Off On

Configure conditions for automatically applying this label

If any of these conditions are met, this label is applied

CONDITION NAME	OCCURRENCES
no condition set	
+ Add a new condition	

- o. You have the ability to choose from pre-defined sensitive information types or you can click custom to type in your own keywords to detect. Here I will search for SSN:

Condition □ ×

T-Minus 365 - Azure Information Protection

Save Discard Delete

Choose the type of condition ⓘ

Information Types
 Custom

Choose an industry

All
 Financial
 Medical and Health
 Privacy

Select information types

NAME

USA Social Security Number (SSN)

* Minimum number of occurrences

Count occurrences with unique values only

Off
 On

Choose the type of condition ⓘ

Information Types
 Custom

* Name

* Match exact phrase or pattern ⓘ

Match as a regular expression

Off
 On

Match with case sensitivity

Off
 On

* Minimum number of occurrences

Count occurrences with unique values only

Off
 On

- p. After you click save, you will see a new button that ask you how you would like to apply the label. If you choose recommended you will be able to write a custom message to the user. If you choose Automatic it will auto-apply

CONDITION NAME	OCCURRENCES
USA Social Security Number (SSN)	1
+ Add a new condition	

Select how this label is applied: automatically or recommended to user

Automatic
 Recommended

Add policy tip describing to users the reason for applying this label

It is recommended to label this file as Encrypt SSN ✓

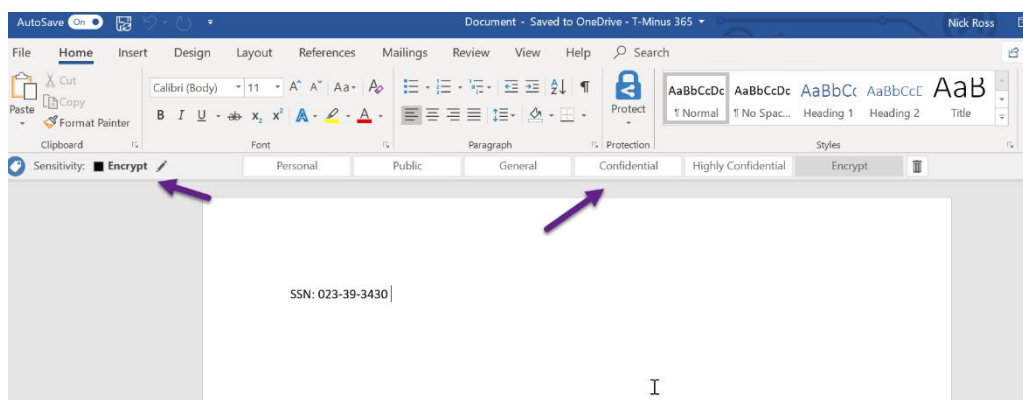
Add notes for administrator use

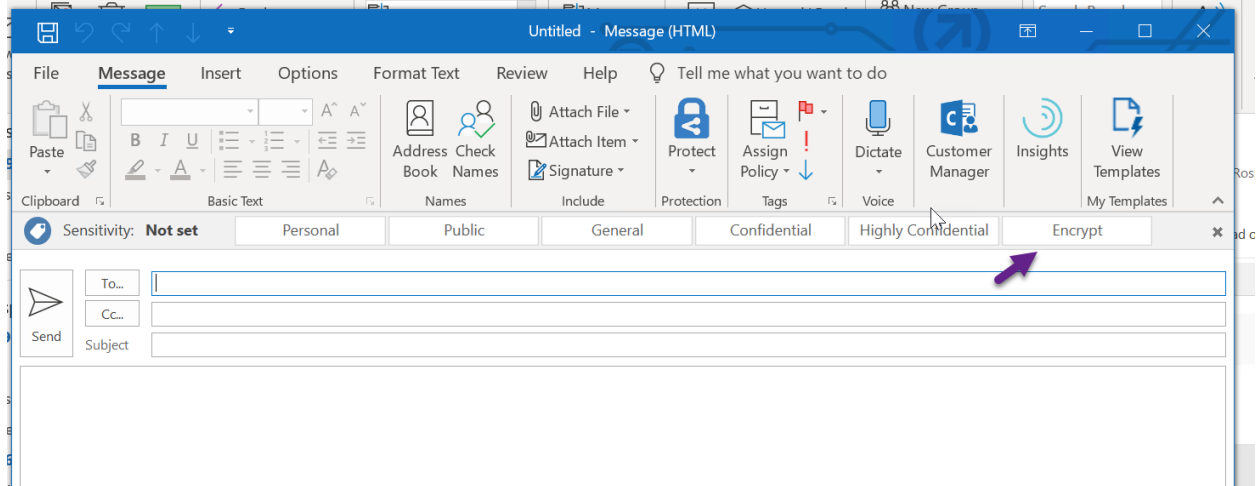
Enter notes for internal housekeeping

- q. After you click save you will now see your new label:

- Personal
- Public
- General
- Confidential
- Highly Confidential
- Test Label
- Encrypt

- r. From here you can select the label to apply to documents and email messages

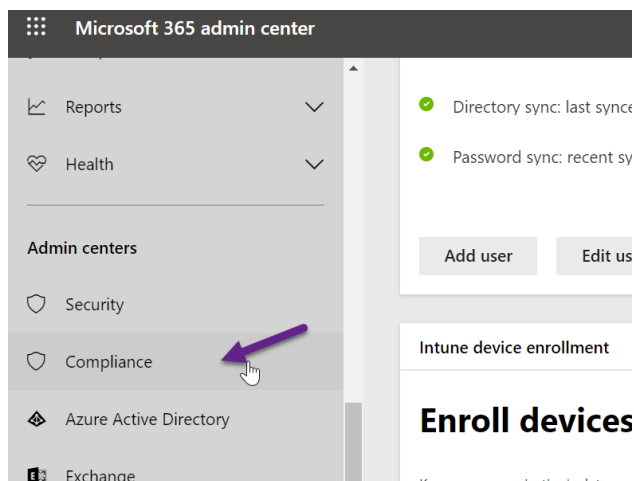




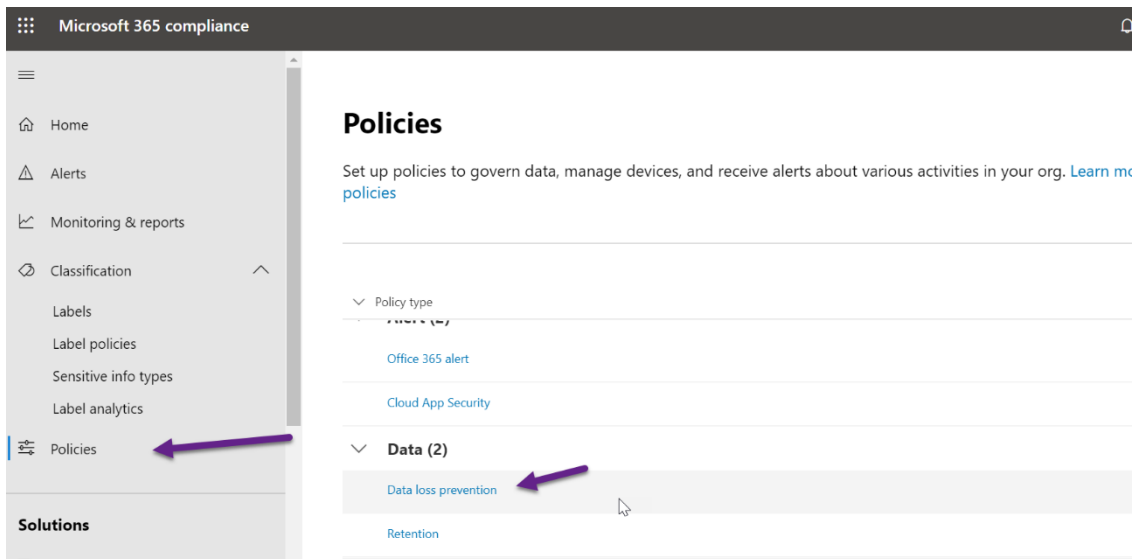
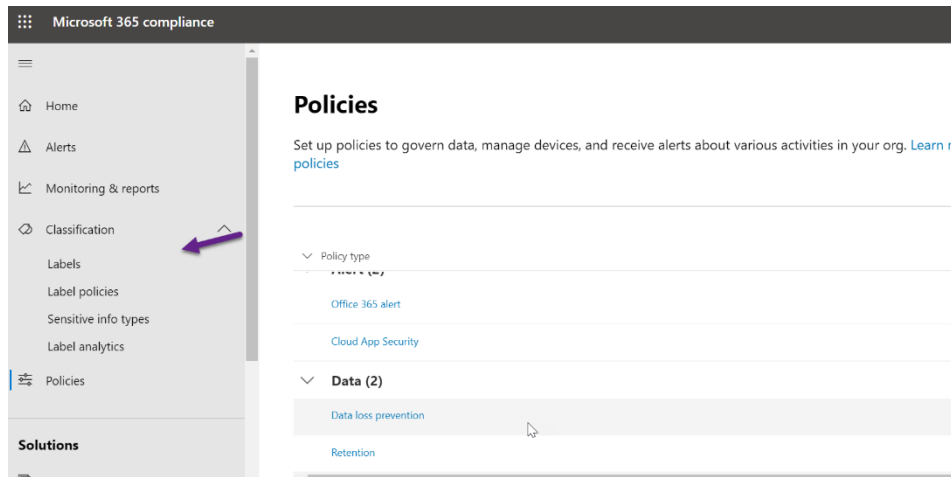
Data Loss Prevention Policies

Within the Compliance center of a tenant, we can configure custom DLP policies that can auto-apply to content across Exchange, OneDrive, SharePoint, and Teams. There are pre-defined templates that relate to certain compliance regulations like HIPAA and FINRA. In this tutorial, we will be configuring a policy for HIPAA.

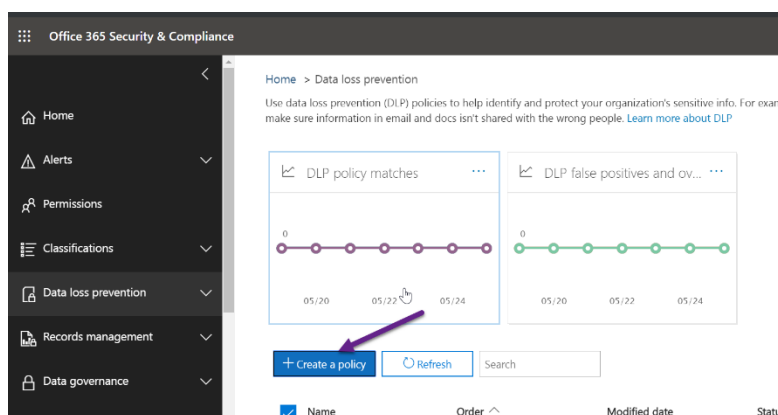
- a. In the admin center for the 365 tenant, click “Compliance” Under admin centers:



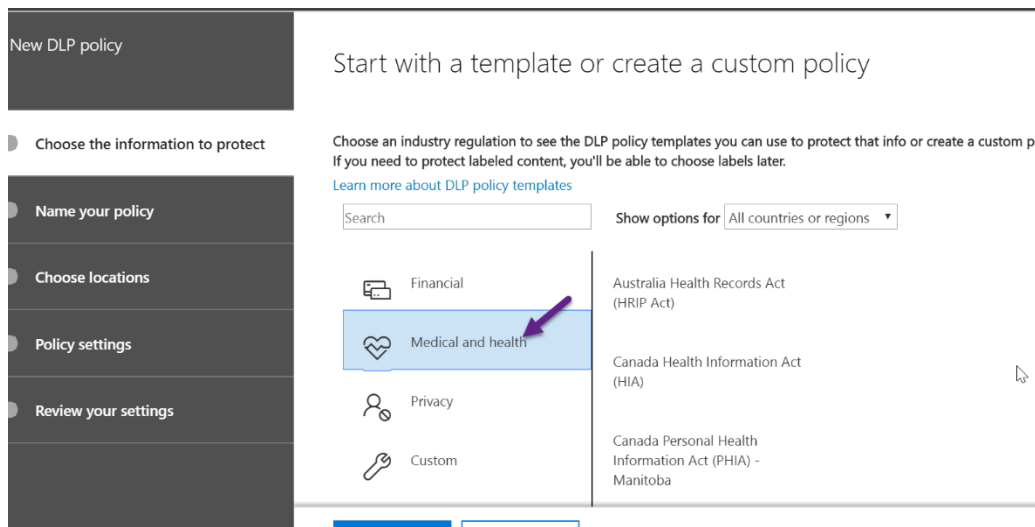
- b. Here we can see the labels we were just looking at as well as the ability to create new policies. Click Policies, then Data loss prevention:



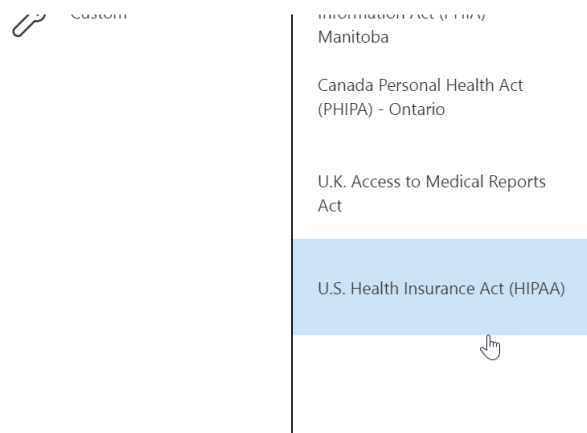
- c. You will be redirected to the Security and Compliance center. Here we can see reports and create new policies. We will click “+ Create a policy”



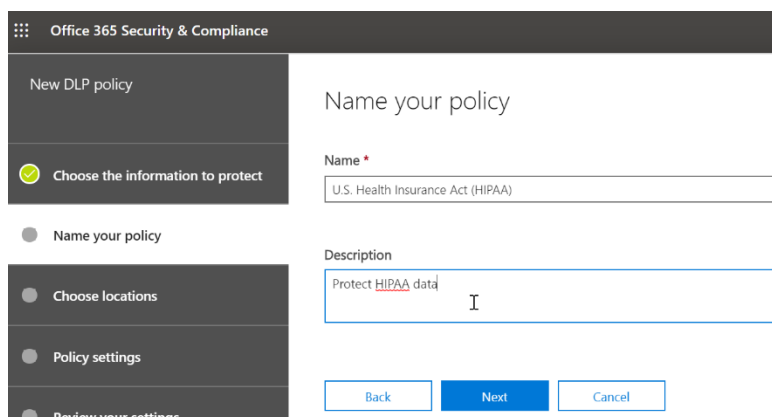
d. We are going to choose “medical” and select “US Health Insurance Act (HIPAA)”



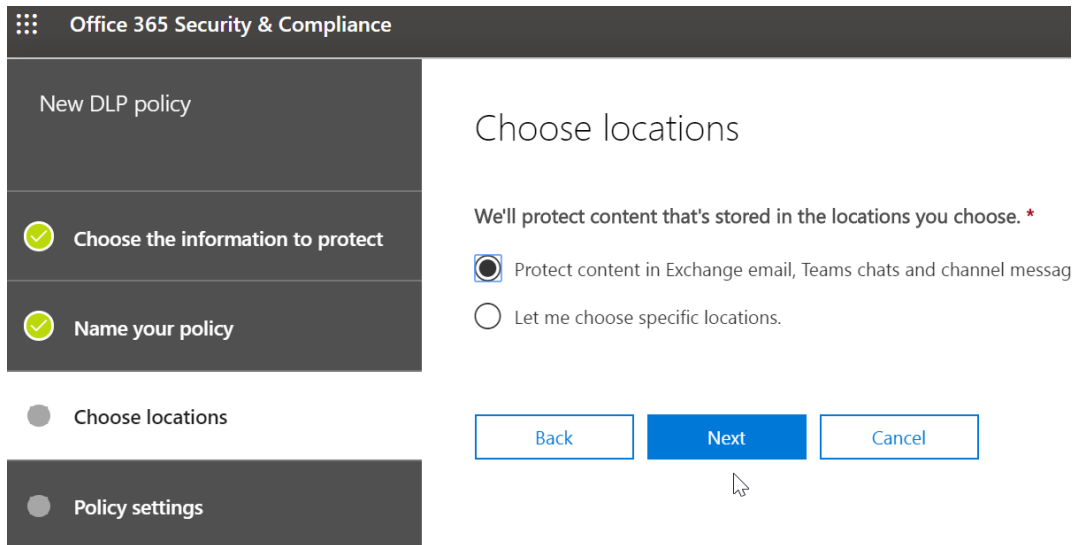
Start with a template or create a custom policy



e. After we click next, we can add a name and description:



- f. You can choose specific locations choosing only exchange for example or selecting all. I will be leaving this defaulted.



Office 365 Security & Compliance

New DLP policy

- ✓ Choose the information to protect
- ✓ Name your policy
- Choose locations
- Policy settings

Choose locations

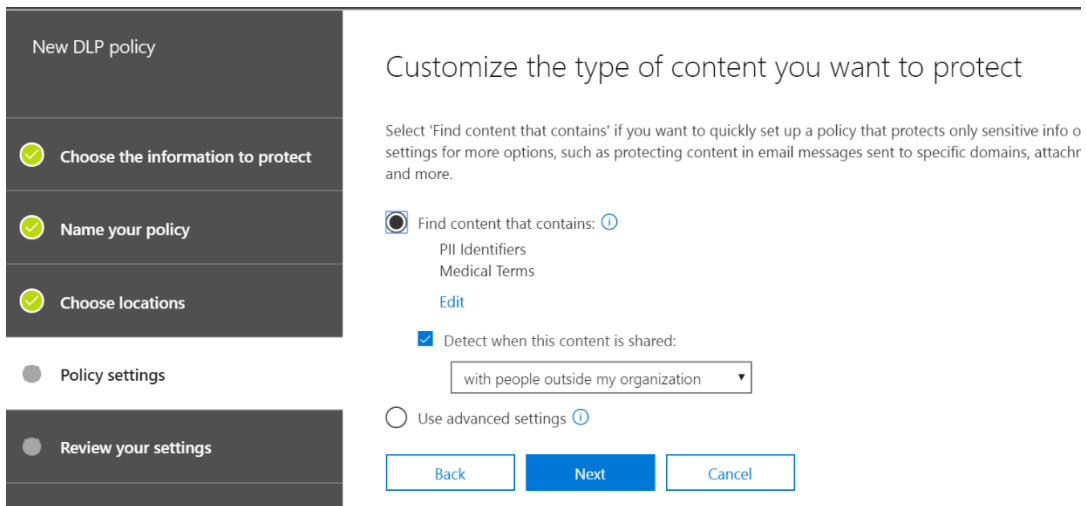
We'll protect content that's stored in the locations you choose.*

Protect content in Exchange email, Teams chats and channel messages

Let me choose specific locations.

Back Next Cancel

- g. Next you can customize the items you want to protect, I am going to leave these settings defaulted.



New DLP policy

- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Choose locations
- Policy settings
- Review your settings

Customize the type of content you want to protect

Select 'Find content that contains' if you want to quickly set up a policy that protects only sensitive info o settings for more options, such as protecting content in email messages sent to specific domains, attachr and more.

Find content that contains: ⓘ

- PII Identifiers
- Medical Terms
- Edit

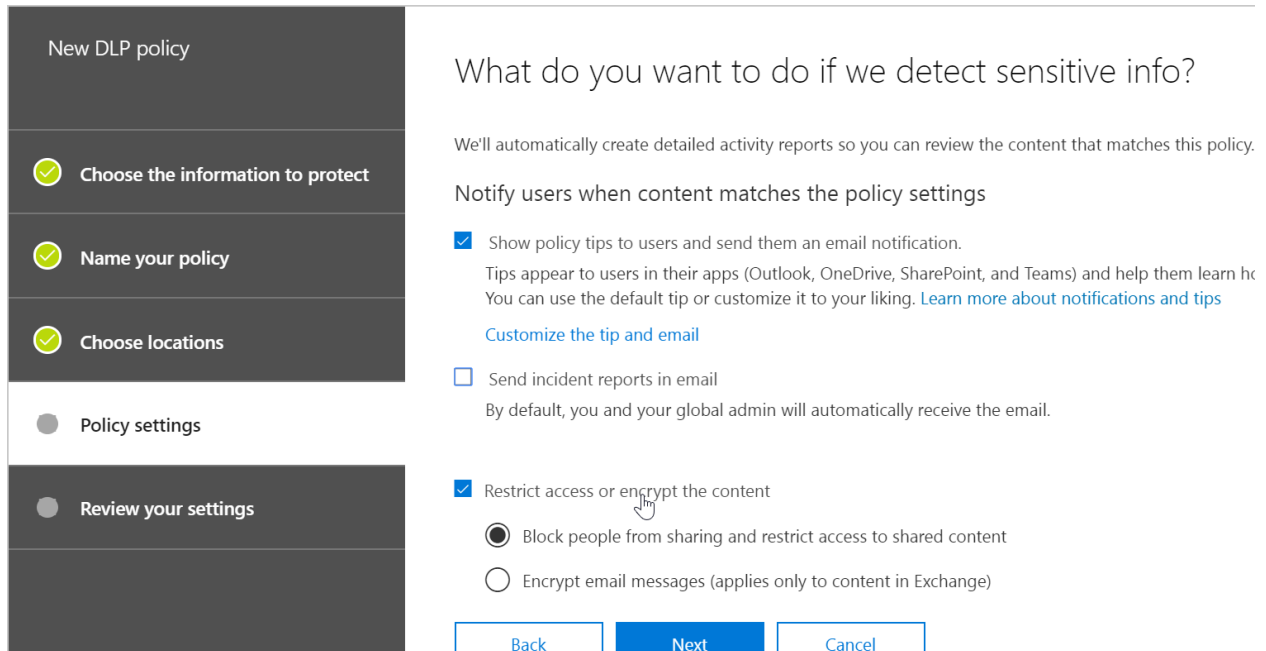
Detect when this content is shared:

with people outside my organization ▾

Use advanced settings ⓘ

Back Next Cancel

- h. Here you can modify the conditions of which action is taken when sensitive content is found.
 NOTE If you choose the encrypt method, this can only apply to exchange. You may want to create 2 separate policies if you want this encryption but also want to apply policies to SharePoint, OneDrive, and Teams



New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings

What do you want to do if we detect sensitive info?

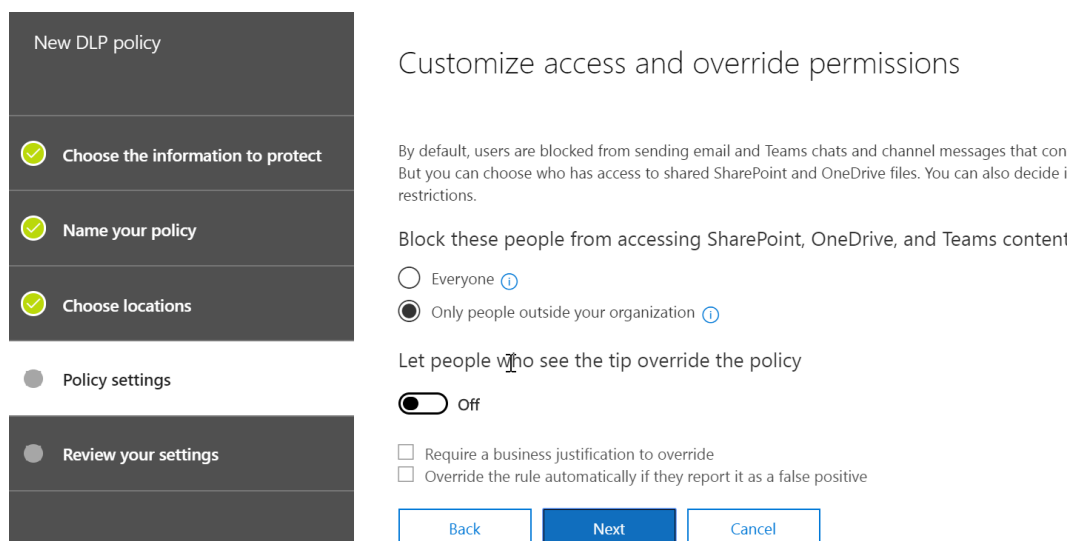
We'll automatically create detailed activity reports so you can review the content that matches this policy.

Notify users when content matches the policy settings

- Show policy tips to users and send them an email notification.
 Tips appear to users in their apps (Outlook, OneDrive, SharePoint, and Teams) and help them learn how to protect sensitive information. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)
[Customize the tip and email](#)
- Send incident reports in email
 By default, you and your global admin will automatically receive the email.
- Restrict access or encrypt the content
 - Block people from sharing and restrict access to shared content
 - Encrypt email messages (applies only to content in Exchange)

[Back](#) [Next](#) [Cancel](#)

- i. Next, we can get even more granular with our settings, blocking outside users from accessing content that contains PII or allowing users to override our policy



New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings

Customize access and override permissions

By default, users are blocked from sending email and Teams chats and channel messages that contain sensitive information. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to allow users to override the policy.

Block these people from accessing SharePoint, OneDrive, and Teams content

- Everyone
- Only people outside your organization

Let people who see the tip override the policy

- Off
- Require a business justification to override
- Override the rule automatically if they report it as a false positive

[Back](#) [Next](#) [Cancel](#)

- j. Lastly, you can decide if you want to test the policy out first before making it GA to the entire tenant

New DLP policy

● Choose the information to protect

● Name your policy

● Choose locations

● Policy settings

● Review your settings

Do you want to turn on the policy or test things out first?

Do you want to turn on the policy right away or test things out first?

Keep in mind that after you turn it on, it'll take up to an hour for the policy to take effect.

Yes, turn it on right away
 I'd like to test it out first
 Show policy tips while in test mode
 No, keep it off. I'll turn it on later.

Back
Next
Cancel

- k. If our settings look ok, we can click create

☰ Office 365 Security & Compliance

New DLP policy

✔ Choose the information to protect

✔ Name your policy

✔ Choose locations

✔ Policy settings

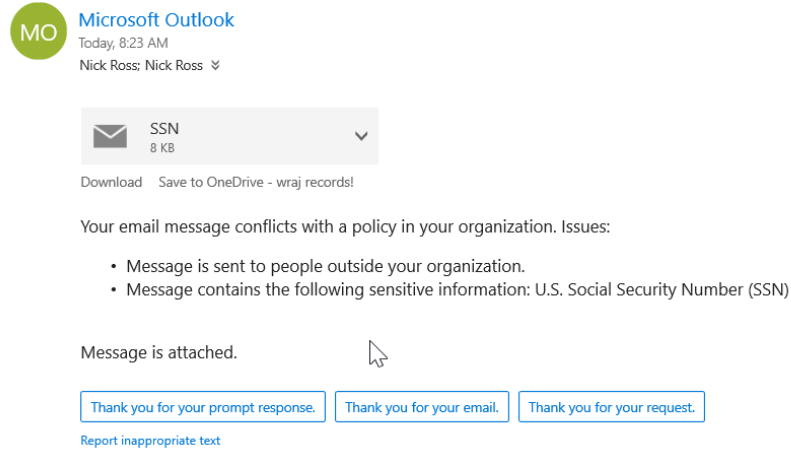
● Review your settings

Review your settings

Template name	U.S. Health Insurance Act (HIPAA)	Edit
Policy name	U.S. Health Insurance Act (HIPAA)	Edit
Description	Protect HIPAA data	Edit
Applies to content in these locations	Exchange email SharePoint sites OneDrive accounts	Edit

- I. If a message is detected with the settings you define, the user will get a message rejection and policy tip. NOTE: if you are testing, only legitimate pieces of sensitive info will trigger the policy

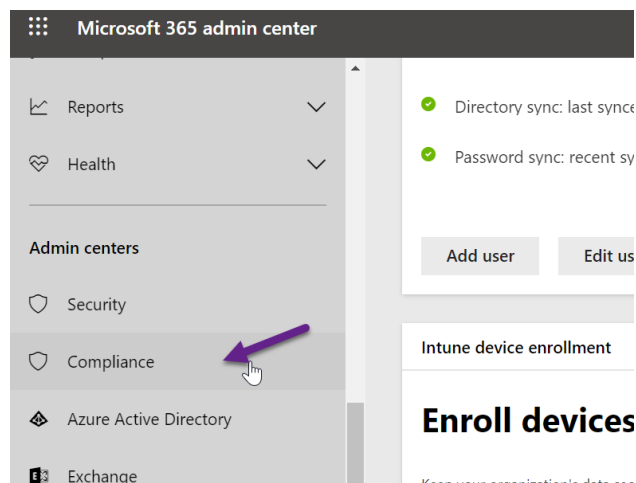
Notification: SSN



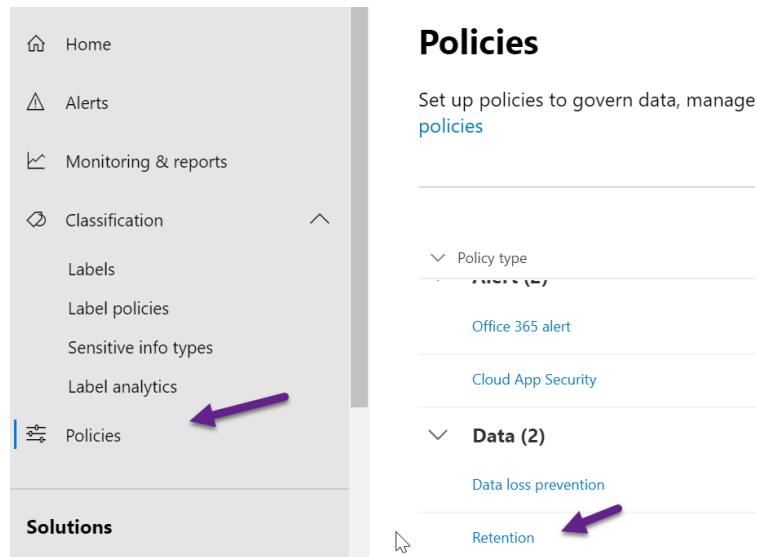
Retention Policies

We can create custom retention policies for certain content in certain locations. By default content is retained for 30 days after deletion. You may want to create custom retention policies for certain content. In this tutorial we are going to be creating custom retention policy for a Teams channel.

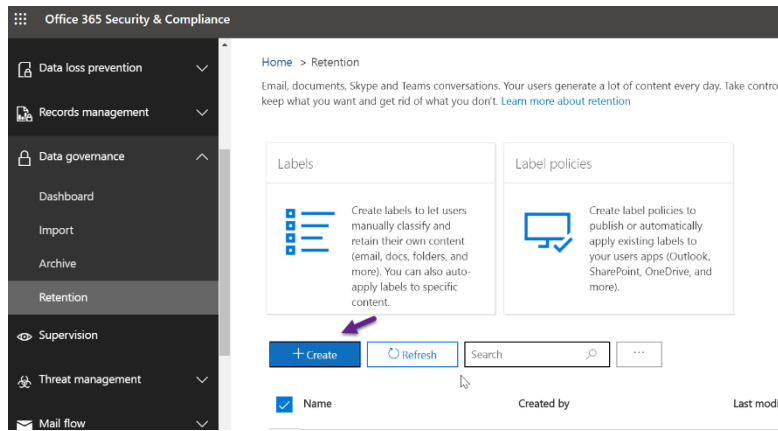
- a. In the admin center for the 365 tenant, click “Compliance” Under admin centers:



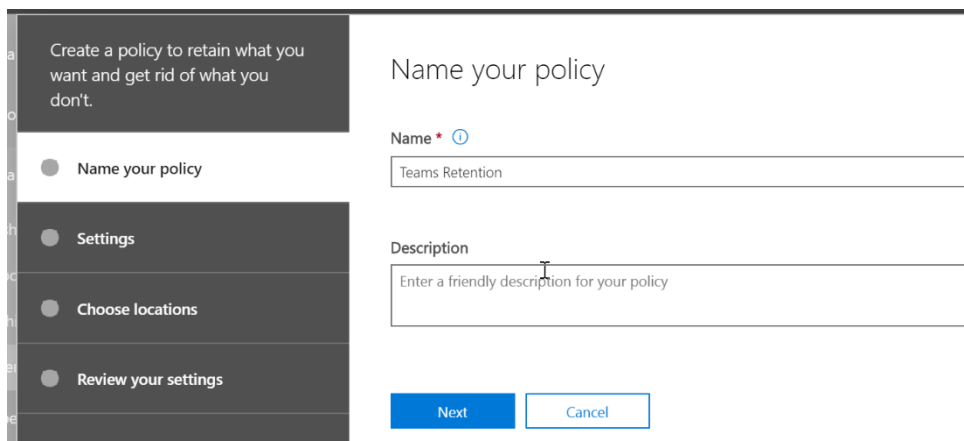
b. Click Policies and Retention



c. You will be redirected to the security and compliance center. Here we can click “+Create”



d. First, we can name our policy and click next



e. Here you can define your settings:

Create a policy to retain what you want and get rid of what you don't.

- Name your policy
- Settings
- Choose locations
- Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... 7 years ⓘ

Forever For this long... based on when it was created ⓘ

Do you want us to delete it after this time? ⓘ

Yes No

No, just delete content that's older than ⓘ

1 years ⓘ

f. Now I will add the Team channel toggle and choose the team I want it to apply to:

Create a policy to retain what you want and get rid of what you don't.

- Name your policy
- Settings
- Choose locations
- Review your settings

Choose locations

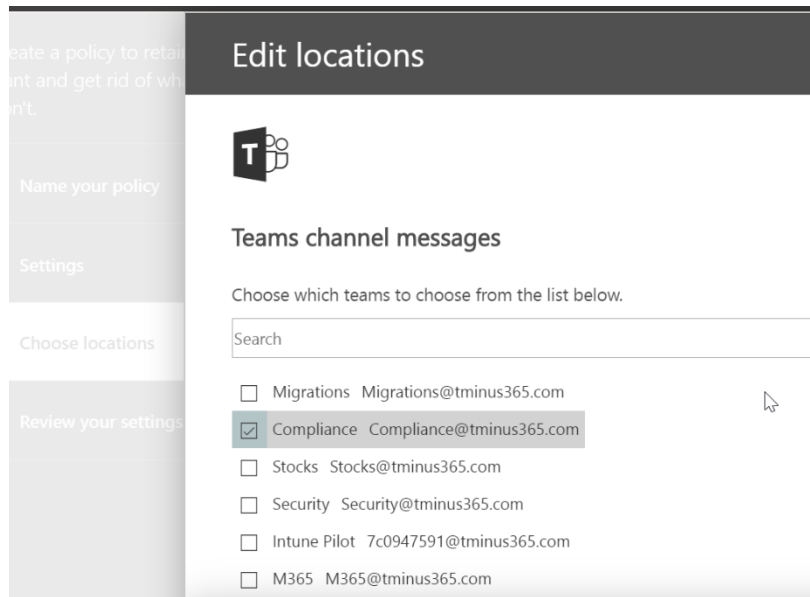
Exchange public folders

Exchange public folders

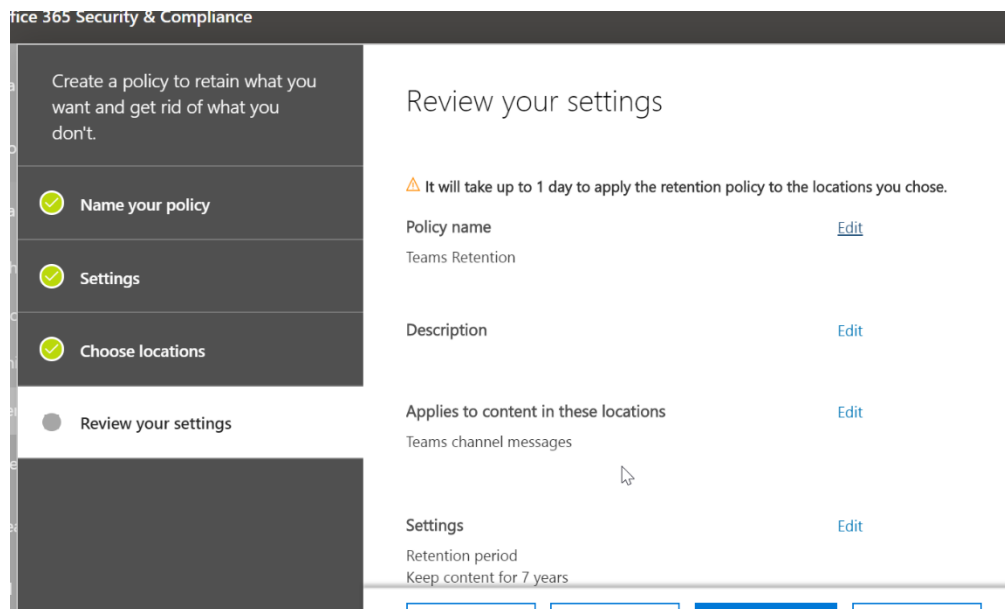
Teams channel messages

All Choose teams Exclude team

Teams chats



g. After I am done reviewing my settings I can select create:



Conclusion

I hope this article provided you some targeted guidance on DLP policies. Any feedback to improve your experience would be greatly appreciated. I would also like to hear if there is more content that you would like to see in this guide. Any feedback can be sent to my email below:

Msp4msps@tminus365.com

