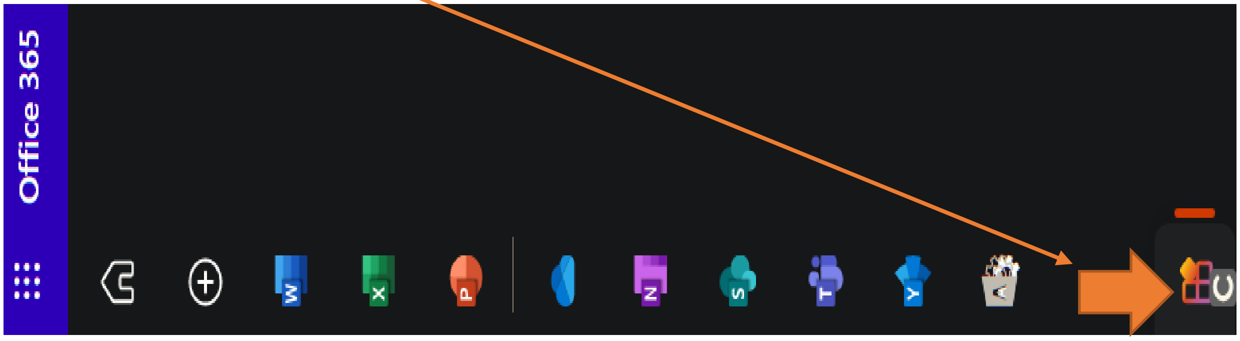
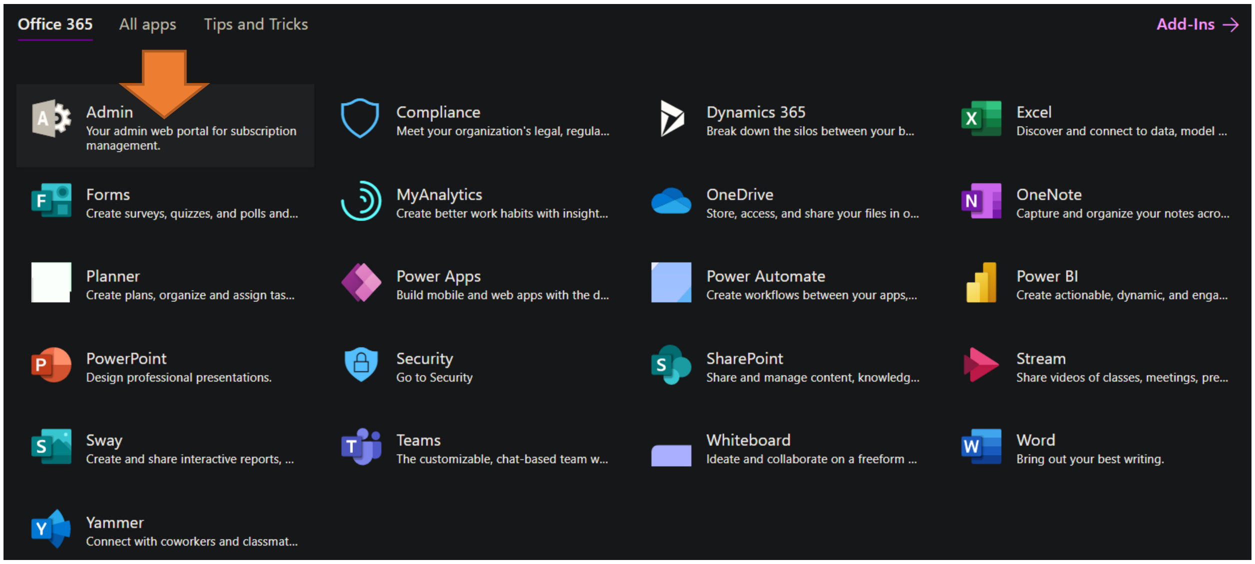
Implementing DLP within Office 365

In this post, I will cover the configuration part of DLP (Data Loss Prevention) within Office 365. Login to Office 365 portal. Click this



Click Admin



Admin
Your admin web portal for subscription management.

Compliance
Meet your organization's legal, regula...

Dynamics 365
Break down the silos between your b...

Excel
Discover and connect to data, model ...

Forms
Create surveys, quizzes, and polls and...

MyAnalytics
Create better work habits with insight...

OneDrive
Store, access, and share your files in o...

OneNote
Capture and organize your notes acro...

Planner
Create plans, organize and assign tas...

Power Apps
Build mobile and web apps with the d...

Power Automate
Create workflows between your apps,...

Power BI
Create actionable, dynamic, and enga...

PowerPoint
Design professional presentations.

Security
Go to Security

SharePoint
Share and manage content, knowledg...

Stream
Share videos of classes, meetings, pre...

Sway
Create and share interactive reports, ...

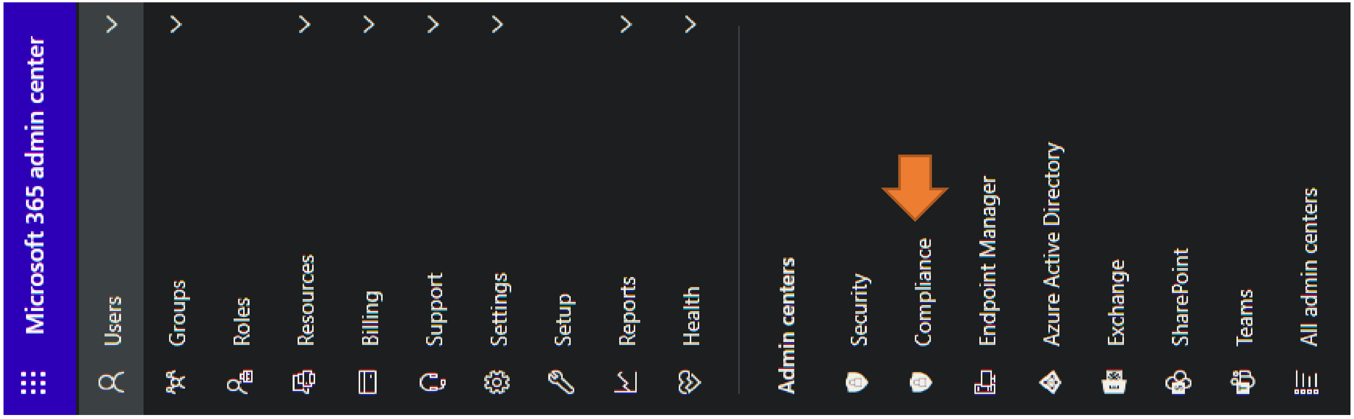
Teams
The customizable, chat-based team w...

Whiteboard
Ideate and collaborate on a freeform ...

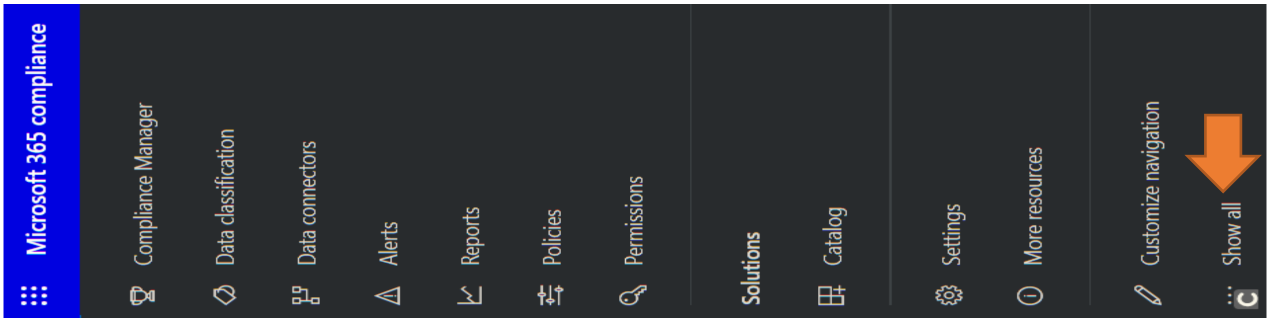
Word
Bring out your best writing.

Yammer
Connect with coworkers and classmat...

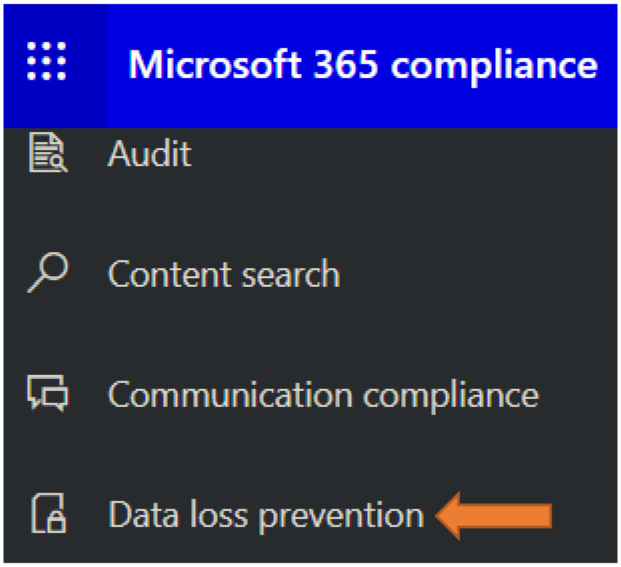
Under Admin Center – Click Compliance

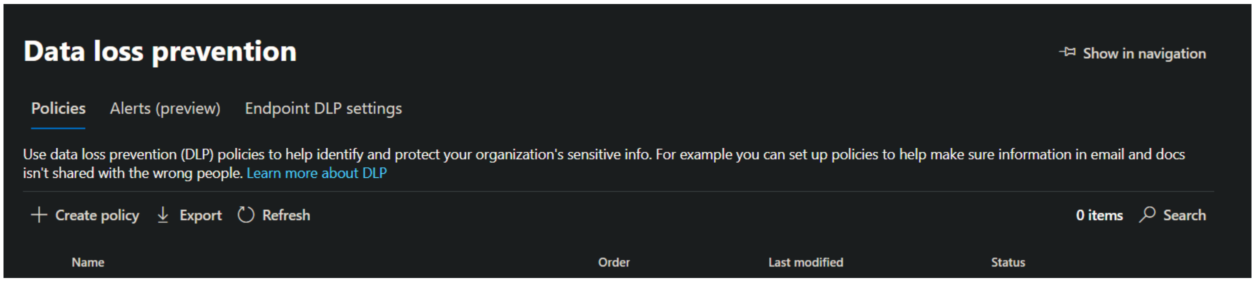


Click Show All



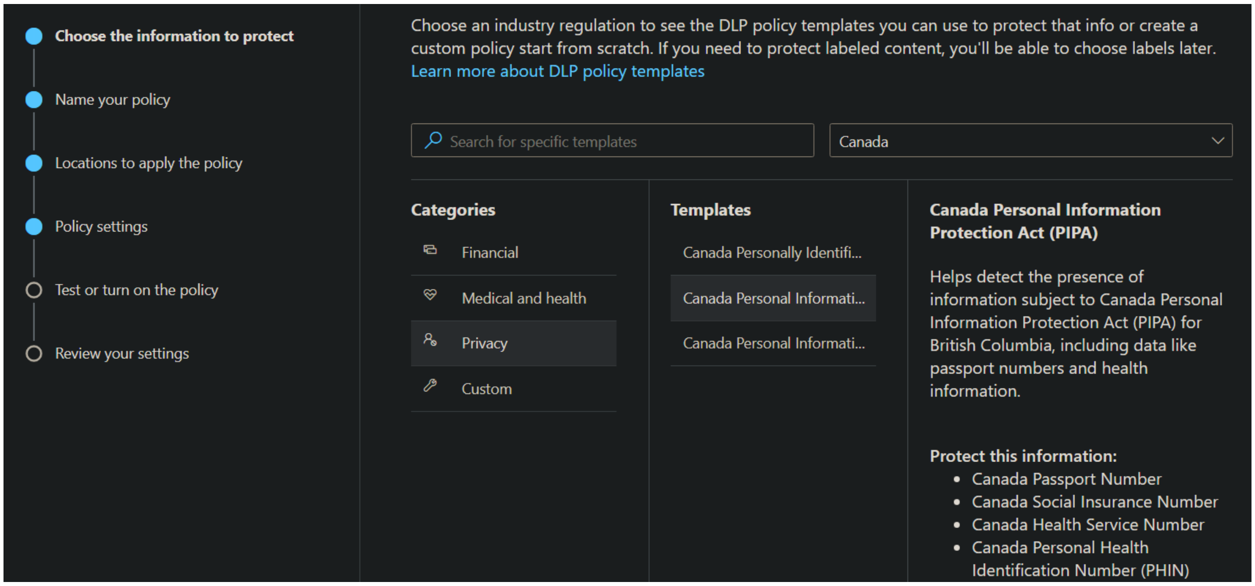
Click Data loss prevention





Data loss prevention

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP


Choose the information to protect
Name your policy
Locations to apply the policy
Policy settings
Test or turn on the policy
Review your settings
Search for specific templates
Canada
Categories
Financial
Medical and health
Privacy
Custom
Templates
Canada Personally Identifi...
Canada Personal Informati...
Canada Personal Informati...

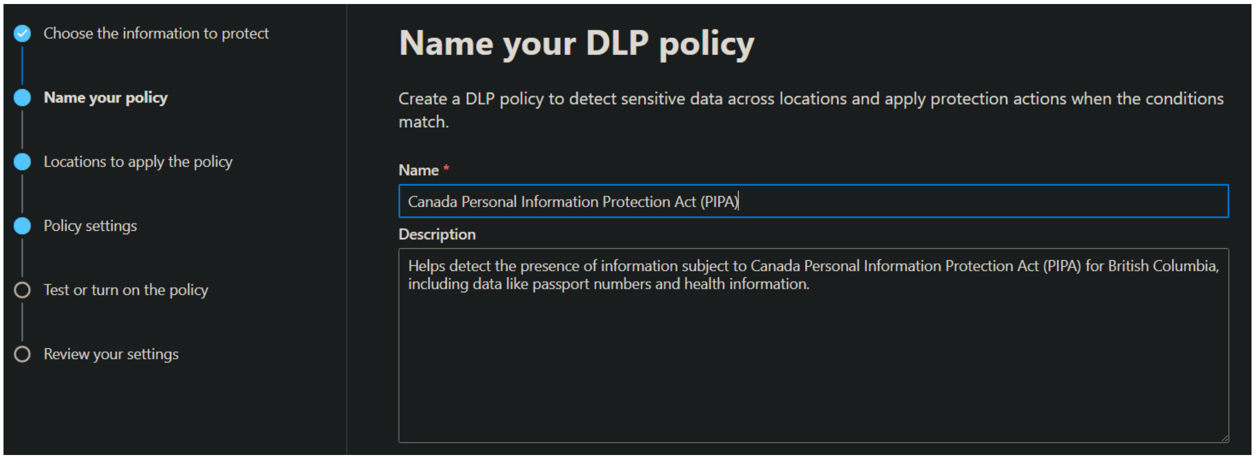
Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP policy templates

Canada Personal Information Protection Act (PIPA)

Helps detect the presence of information subject to Canada Personal Information Protection Act (PIPA) for British Columbia, including data like passport numbers and health information.

Protect this information:

- Canada Passport Number
- Canada Social Insurance Number
- Canada Health Service Number
- Canada Personal Health Identification Number (PHIN)

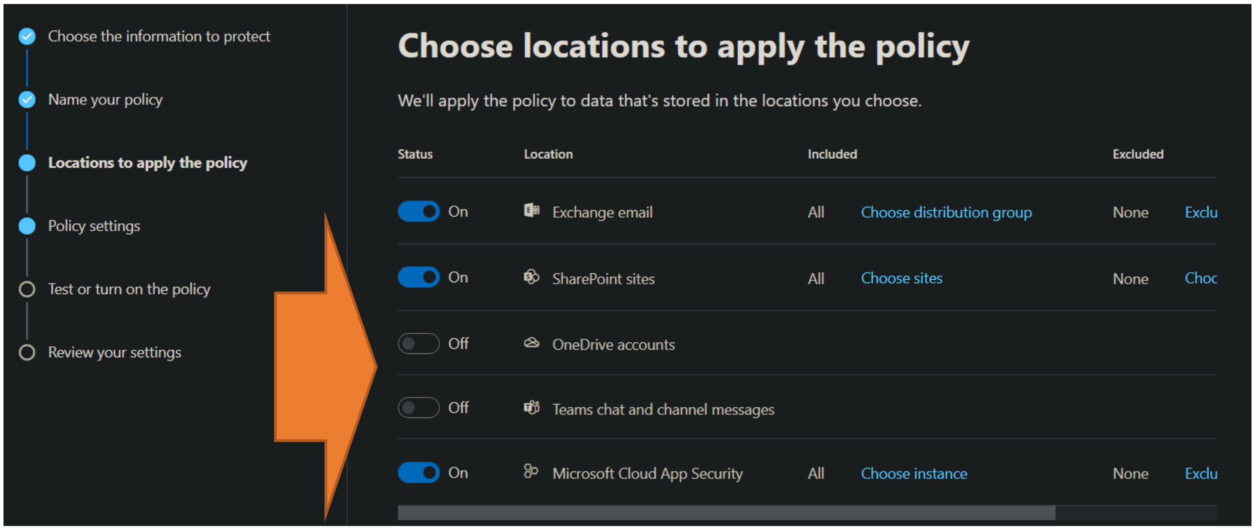

Choose the information to protect
Name your policy
Locations to apply the policy
Policy settings
Test or turn on the policy
Review your settings

Name your DLP policy

Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.

Name *
Canada Personal Information Protection Act (PIPA)

Description
Helps detect the presence of information subject to Canada Personal Information Protection Act (PIPA) for British Columbia, including data like passport numbers and health information.

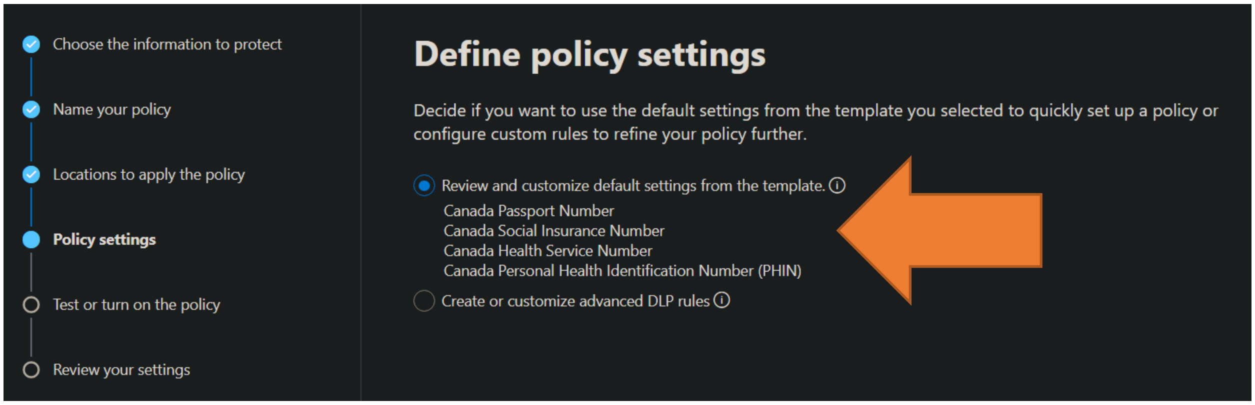


- Choose the information to protect
- Name your policy
- **Locations to apply the policy**
- Policy settings
- Test or turn on the policy
- Review your settings

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Status	Location	Included		Excluded	
On	Exchange email	All	Choose distribution group	None	Exclu
On	SharePoint sites	All	Choose sites	None	Choc
Off	OneDrive accounts				
Off	Teams chat and channel messages				
On	Microsoft Cloud App Security	All	Choose instance	None	Exclu



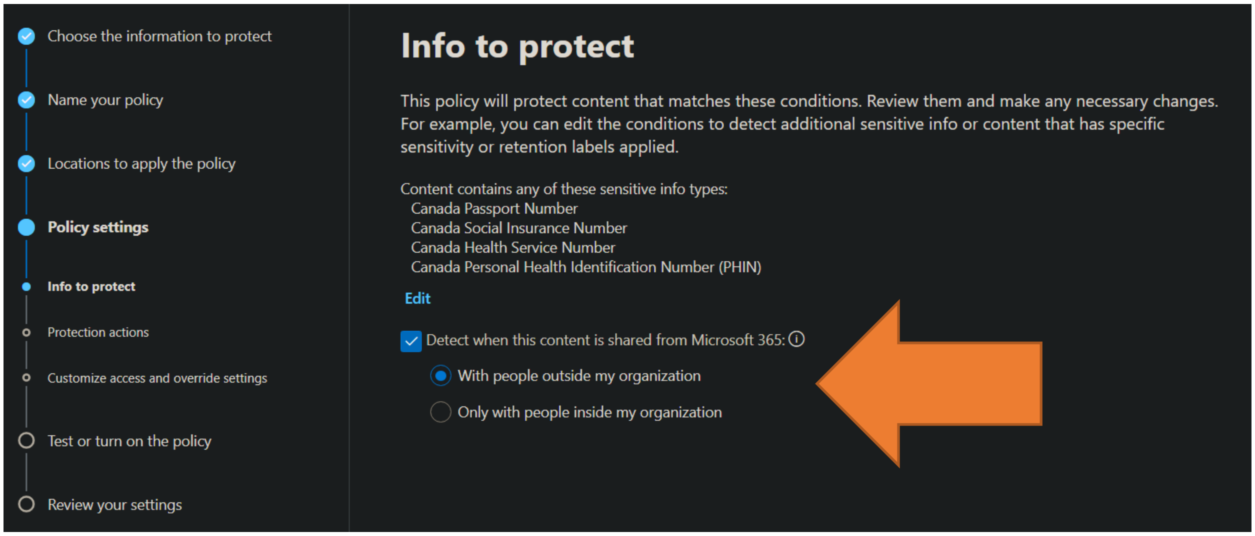
- Choose the information to protect
- Name your policy
- Locations to apply the policy
- **Policy settings**
- Test or turn on the policy
- Review your settings

Define policy settings

Decide if you want to use the default settings from the template you selected to quickly set up a policy or configure custom rules to refine your policy further.

● Review and customize default settings from the template. ⓘ
Canada Passport Number
Canada Social Insurance Number
Canada Health Service Number
Canada Personal Health Identification Number (PHIN)

○ Create or customize advanced DLP rules ⓘ



- Choose the information to protect
- Name your policy
- Locations to apply the policy
- **Policy settings**
  - **Info to protect**
  - Protection actions
  - Customize access and override settings
- Test or turn on the policy
- Review your settings

Info to protect

This policy will protect content that matches these conditions. Review them and make any necessary changes. For example, you can edit the conditions to detect additional sensitive info or content that has specific sensitivity or retention labels applied.

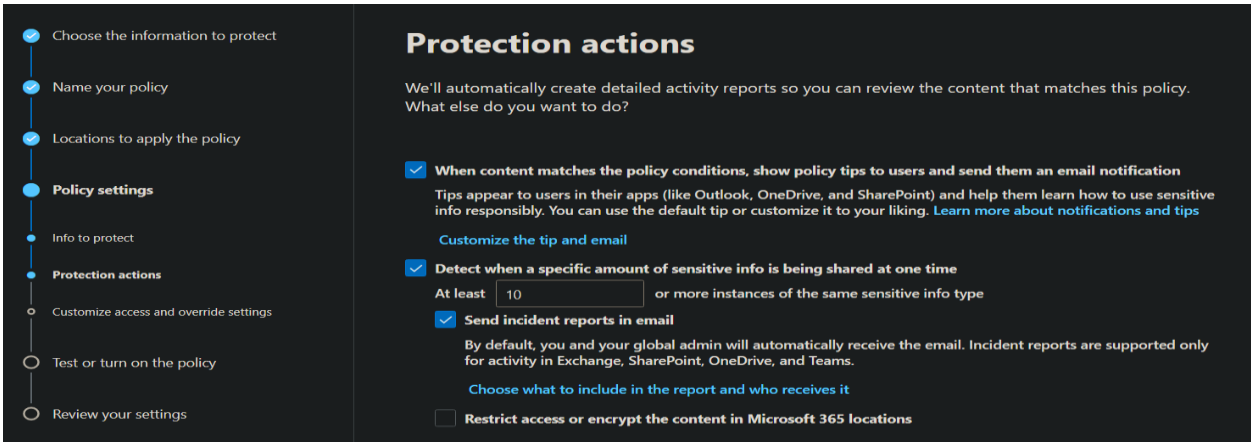
Content contains any of these sensitive info types:
Canada Passport Number
Canada Social Insurance Number
Canada Health Service Number
Canada Personal Health Identification Number (PHIN)

Edit

☑ Detect when this content is shared from Microsoft 365: ⓘ

● With people outside my organization

○ Only with people inside my organization



- Choose the information to protect
- Name your policy
- Locations to apply the policy
- **Policy settings**
  - Info to protect
  - **Protection actions**
  - Customize access and override settings
- Test or turn on the policy
- Review your settings

Protection actions

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

☑ **When content matches the policy conditions, show policy tips to users and send them an email notification**

Tips appear to users in their apps (like Outlook, OneDrive, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. Learn more about notifications and tips

Customize the tip and email

☑ **Detect when a specific amount of sensitive info is being shared at one time**

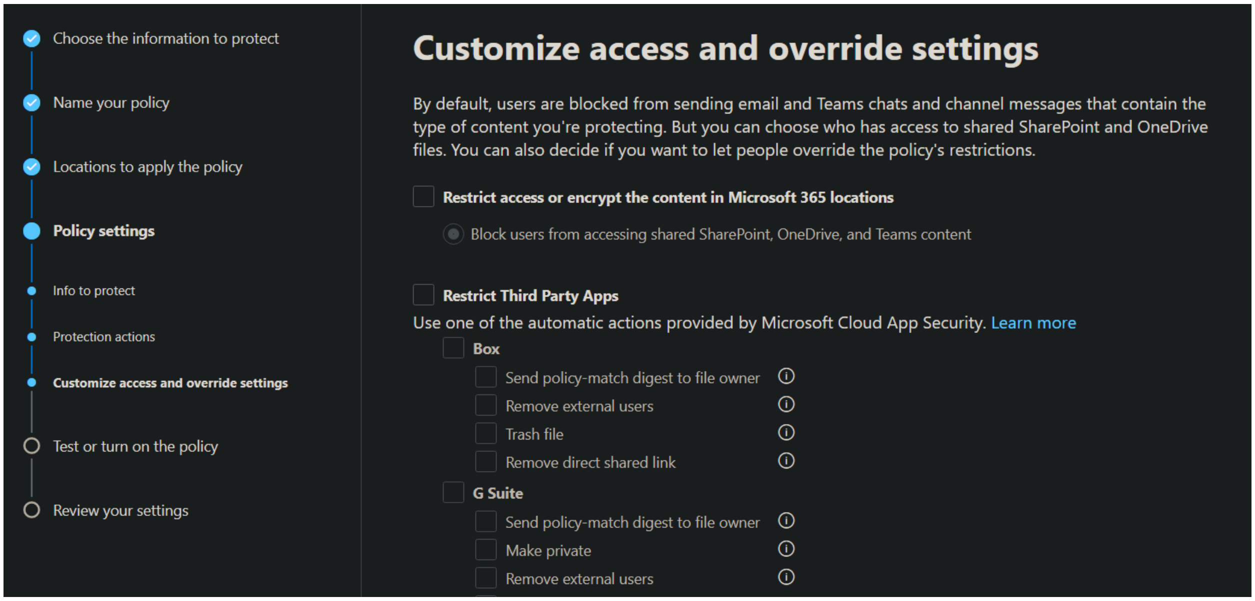
At least 10 or more instances of the same sensitive info type

☑ **Send incident reports in email**

By default, you and your global admin will automatically receive the email. Incident reports are supported only for activity in Exchange, SharePoint, OneDrive, and Teams.

Choose what to include in the report and who receives it

□ **Restrict access or encrypt the content in Microsoft 365 locations**


Choose the information to protect
Name your policy
Locations to apply the policy
Policy settings
Info to protect
Protection actions
Customize access and override settings
Test or turn on the policy
Review your settings

Customize access and override settings

By default, users are blocked from sending email and Teams chats and channel messages that contain the type of content you're protecting. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to let people override the policy's restrictions.

□ **Restrict access or encrypt the content in Microsoft 365 locations**

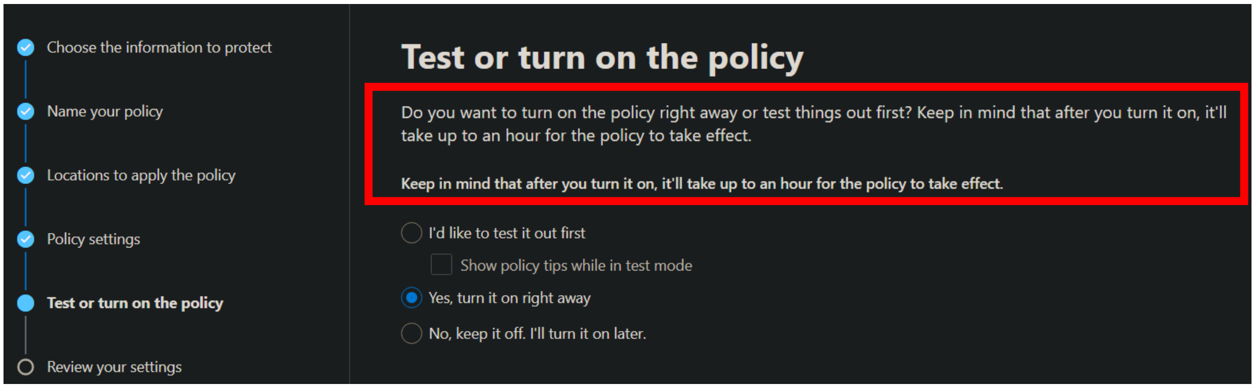
○ Block users from accessing shared SharePoint, OneDrive, and Teams content

□ **Restrict Third Party Apps**

Use one of the automatic actions provided by Microsoft Cloud App Security. Learn more

□ **Box**
- □ Send policy-match digest to file owner ⓘ
- □ Remove external users ⓘ
- □ Trash file ⓘ
- □ Remove direct shared link ⓘ

□ **G Suite**
- □ Send policy-match digest to file owner ⓘ
- □ Make private ⓘ
- □ Remove external users ⓘ


Choose the information to protect
Name your policy
Locations to apply the policy
Policy settings
Test or turn on the policy
Review your settings

Test or turn on the policy

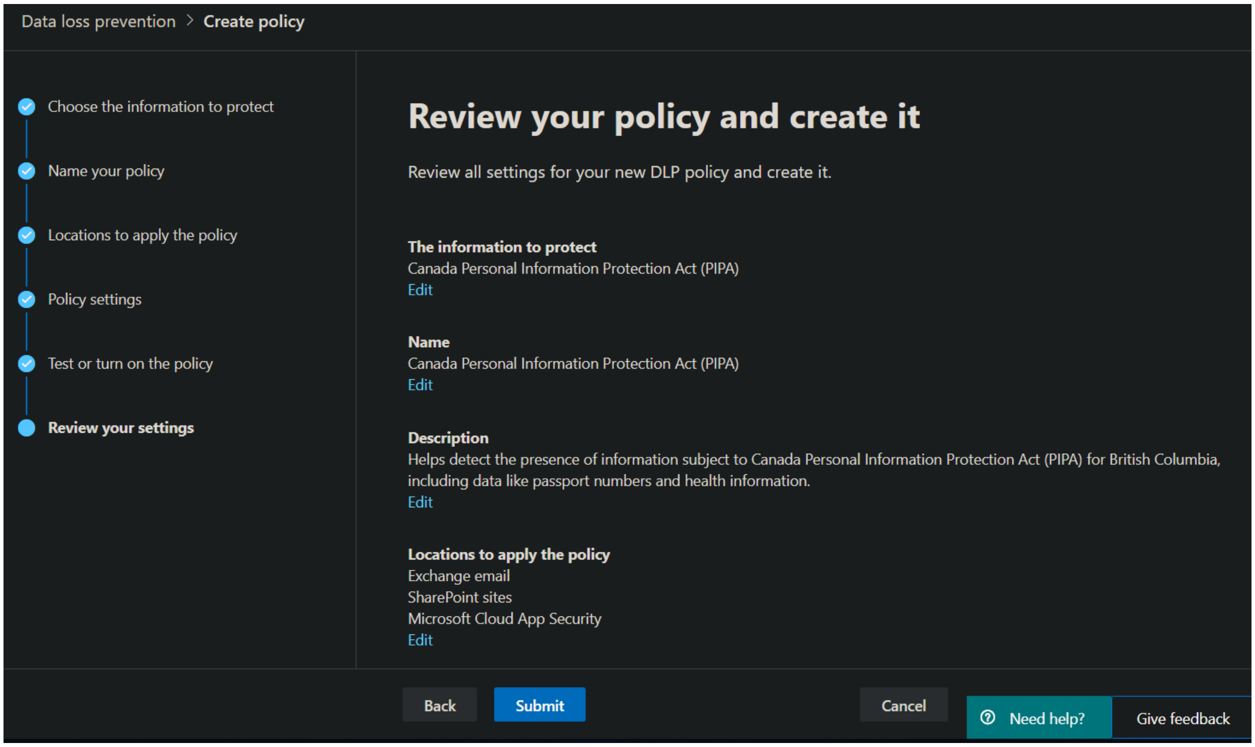
Do you want to turn on the policy right away or test things out first? Keep in mind that after you turn it on, it'll take up to an hour for the policy to take effect.

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

○ I'd like to test it out first
- □ Show policy tips while in test mode

● Yes, turn it on right away

○ No, keep it off. I'll turn it on later.


Data loss prevention > Create policy
Choose the information to protect
Name your policy
Locations to apply the policy
Policy settings
Test or turn on the policy
Review your settings

Review your policy and create it

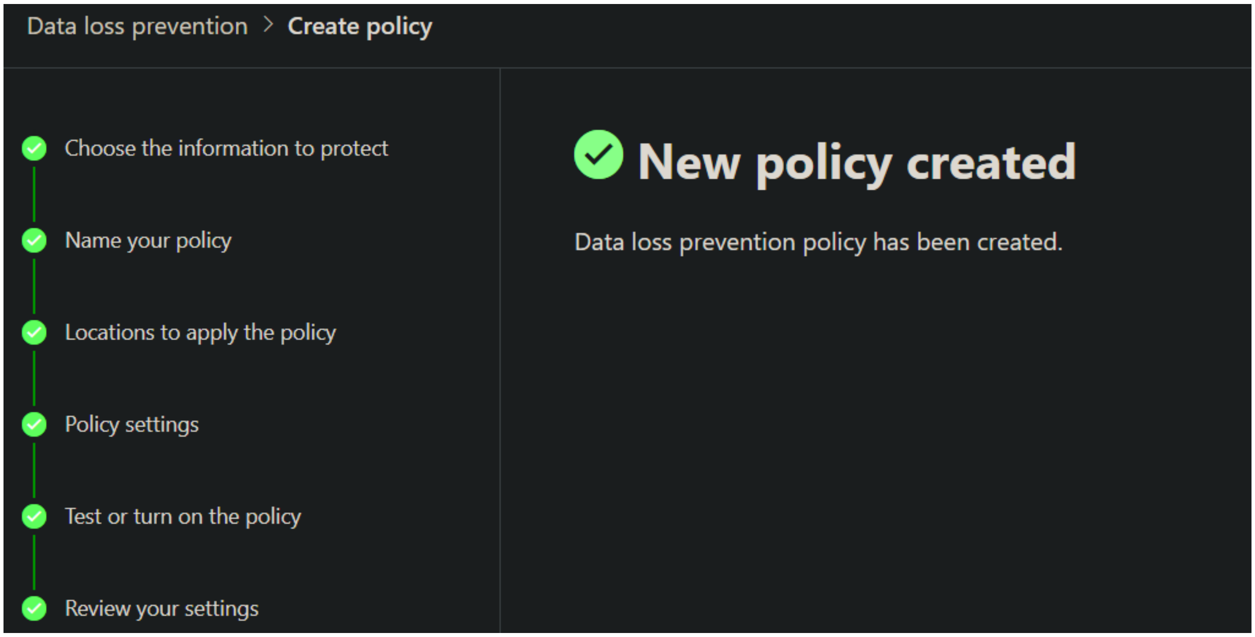
Review all settings for your new DLP policy and create it.

The information to protect
Canada Personal Information Protection Act (PIPA)
Edit

Name
Canada Personal Information Protection Act (PIPA)
Edit

Description
Helps detect the presence of information subject to Canada Personal Information Protection Act (PIPA) for British Columbia, including data like passport numbers and health information.
Edit

Locations to apply the policy
Exchange email
SharePoint sites
Microsoft Cloud App Security
Edit

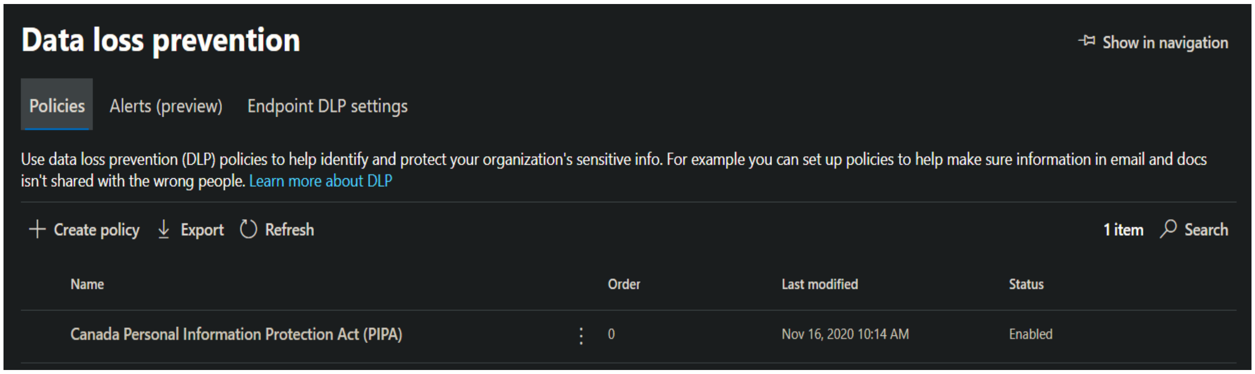


Data loss prevention > Create policy

- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Locations to apply the policy
- ✓ Policy settings
- ✓ Test or turn on the policy
- ✓ Review your settings

✓ New policy created

Data loss prevention policy has been created.

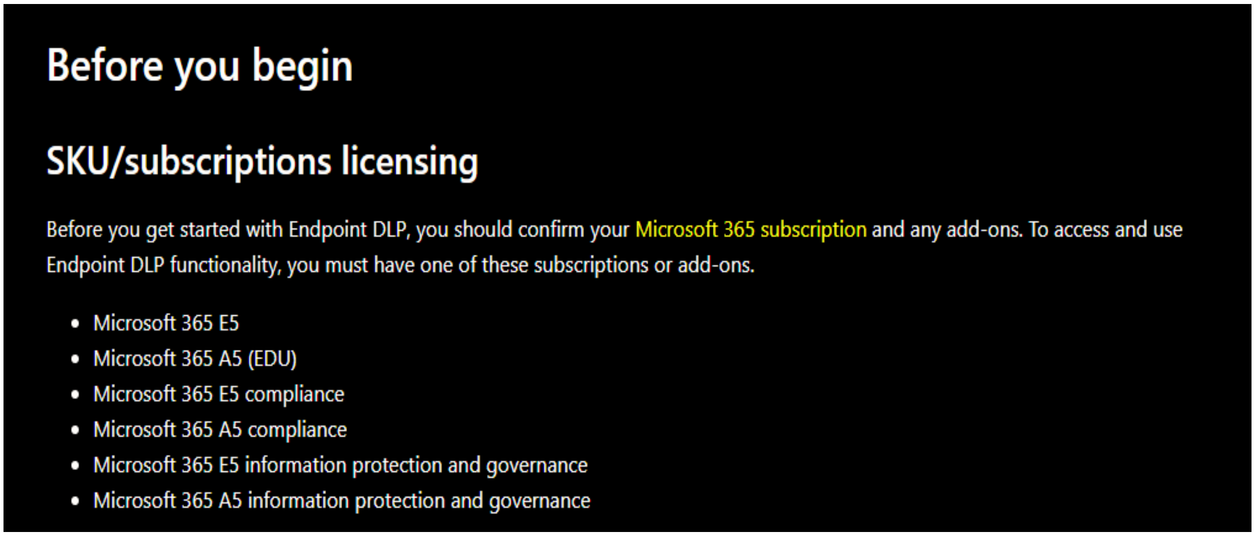


Data loss prevention

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

Name	Order	Last modified	Status
Canada Personal Information Protection Act (PIPA)	0	Nov 16, 2020 10:14 AM	Enabled

Now it is time to test our DLP policy. First up we need to create some sensitive data. Since I have applied Canadian PIPA policy I need to generate some information about health card or passport details to trigger the DLP policy. Please note licensing requirements for DLP/MS 365.



Before you begin

SKU/subscriptions licensing

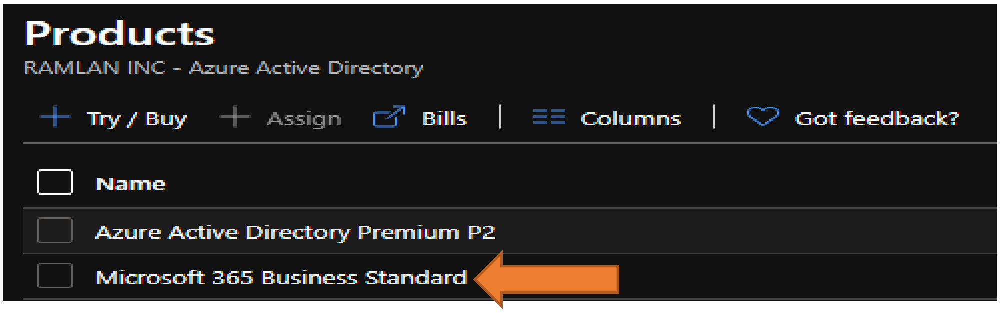
Before you get started with Endpoint DLP, you should confirm your Microsoft 365 subscription and any add-ons. To access and use Endpoint DLP functionality, you must have one of these subscriptions or add-ons.

- Microsoft 365 E5
- Microsoft 365 A5 (EDU)
- Microsoft 365 E5 compliance
- Microsoft 365 A5 compliance
- Microsoft 365 E5 information protection and governance
- Microsoft 365 A5 information protection and governance

You can visit below link for more information about DLP configuration, deployment and auditing.

https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

Since, I have MS 365 Business Standard License, I cannot trigger DLP policy to go into effect.



Products

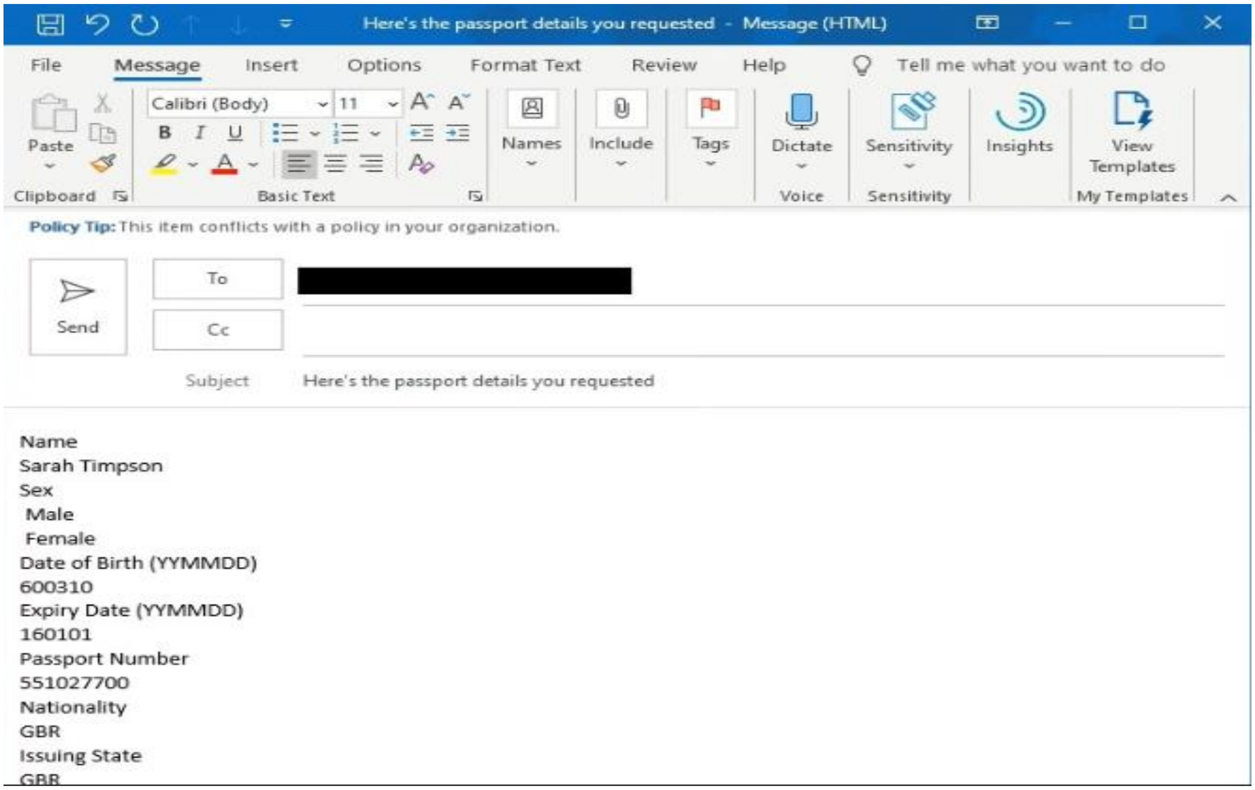
RAMLAN INC - Azure Active Directory

□ Name

□ Azure Active Directory Premium P2

□ Microsoft 365 Business Standard

You get the idea on how to configure and deploy DLP. I am providing few screenshots from MS Site. When you create email with sensitive data this is what you will see.



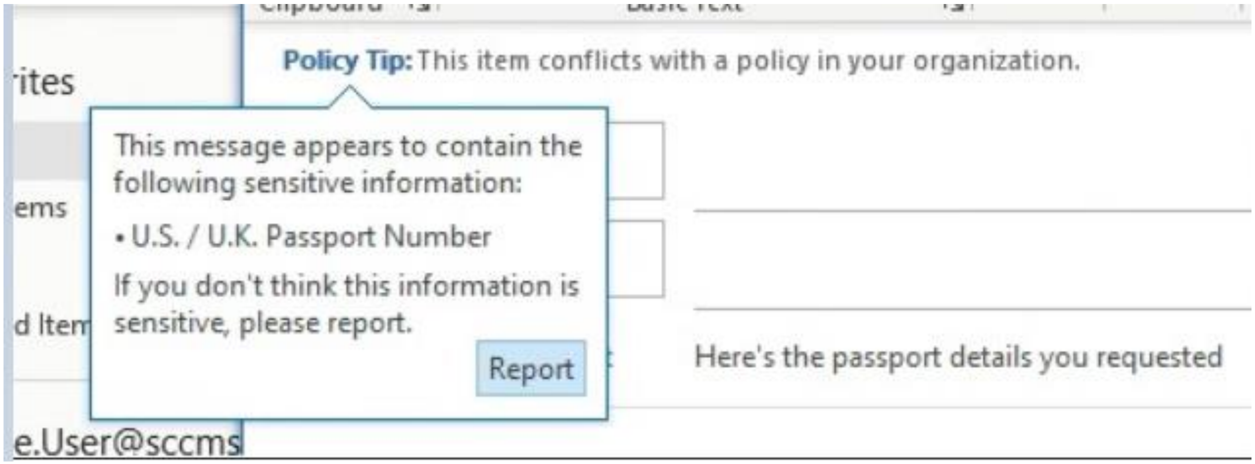
Here's the passport details you requested - Message (HTML)

Policy Tip: This item conflicts with a policy in your organization.

To: [redacted]

Subject: Here's the passport details you requested

Name
Sarah Timpson
Sex
Male
Female
Date of Birth (YYMMDD)
600310
Expiry Date (YYMMDD)
160101
Passport Number
551027700
Nationality
GBR
Issuing State
GBR



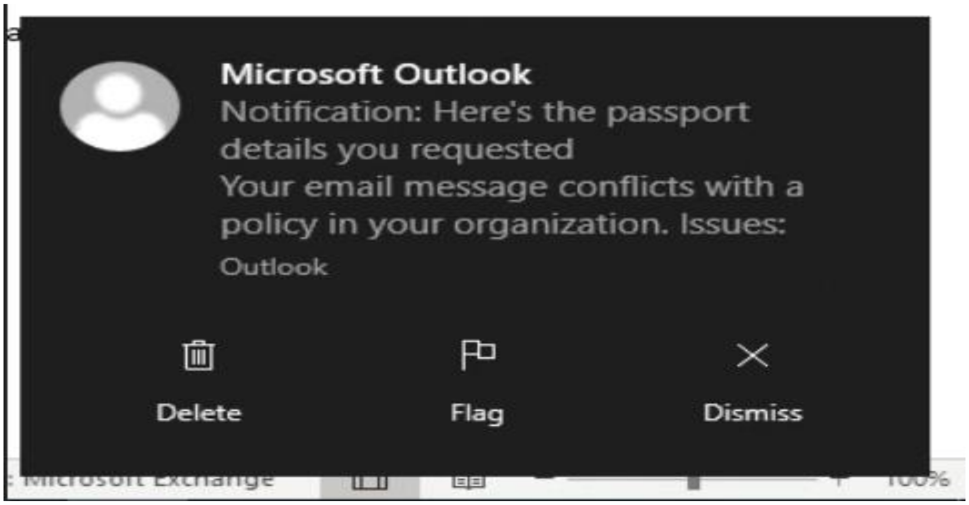
Policy Tip: This item conflicts with a policy in your organization.

This message appears to contain the following sensitive information:

- U.S. / U.K. Passport Number

If you don't think this information is sensitive, please report.

Here's the passport details you requested

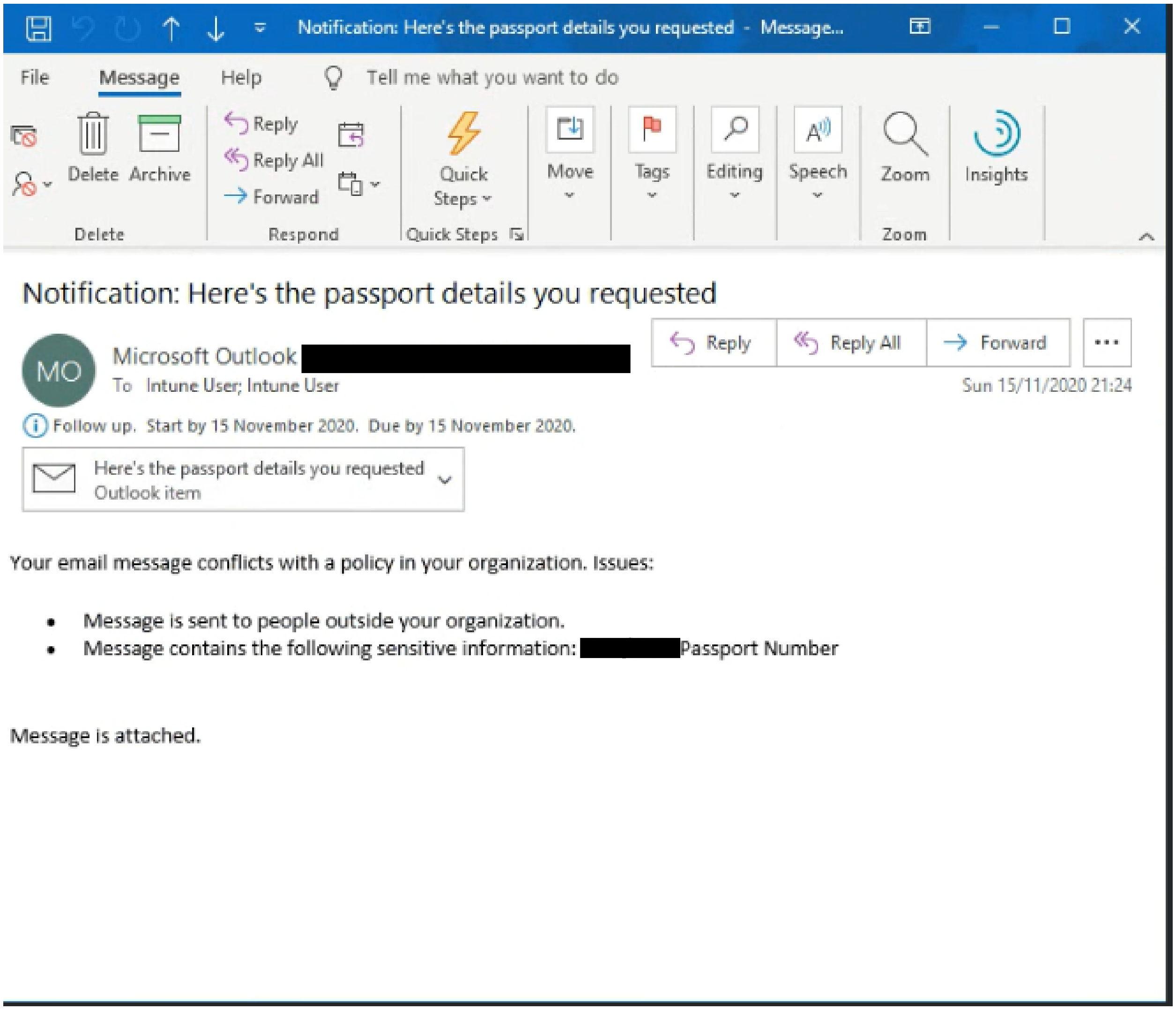


Microsoft Outlook

Notification: Here's the passport details you requested

Your email message conflicts with a policy in your organization. Issues:

Outlook



Notification: Here's the passport details you requested

MO Microsoft Outlook [redacted]

To Intune User; Intune User

Sun 15/11/2020 21:24

Follow up. Start by 15 November 2020. Due by 15 November 2020.

Here's the passport details you requested
Outlook item

Your email message conflicts with a policy in your organization. Issues:

- Message is sent to people outside your organization.
- Message contains the following sensitive information: [redacted]Passport Number

Message is attached.

Thanks

Ram Lan
16th Nov 2020