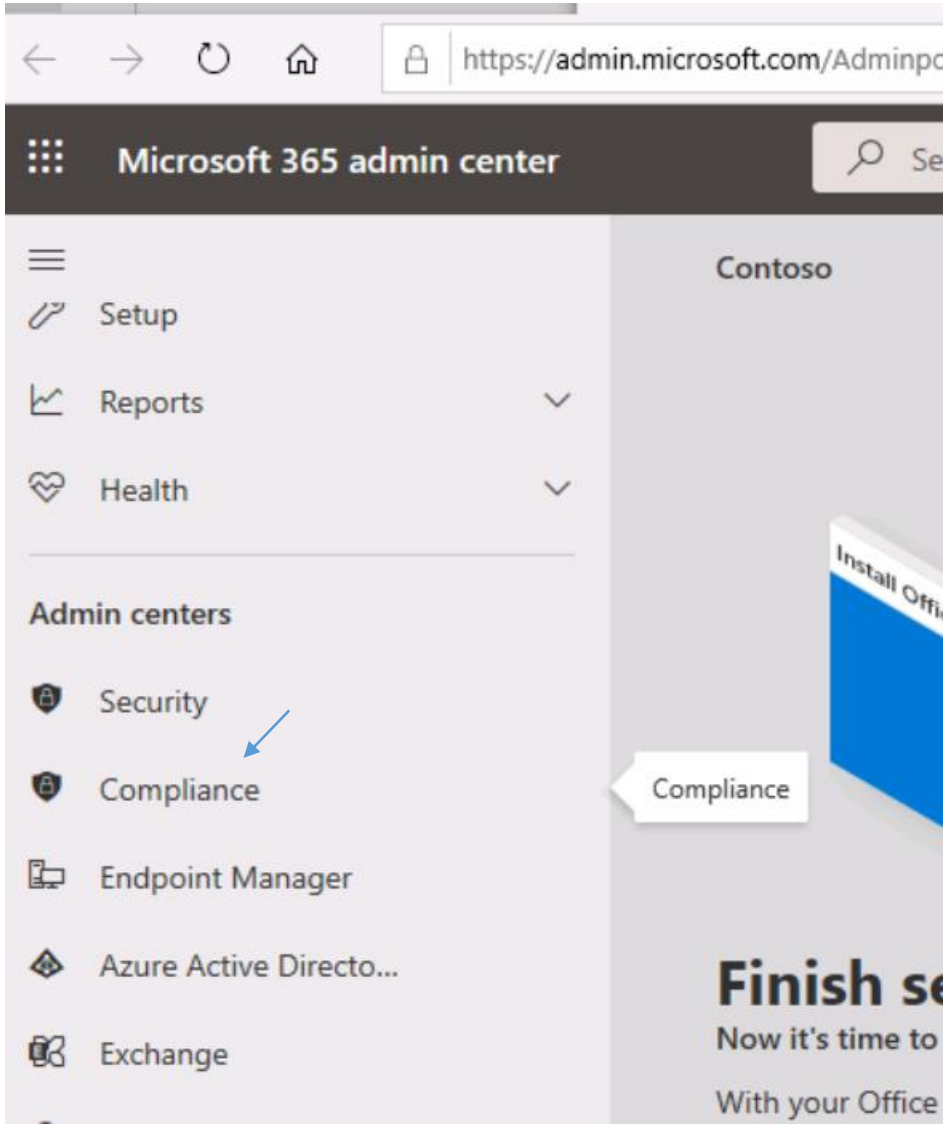
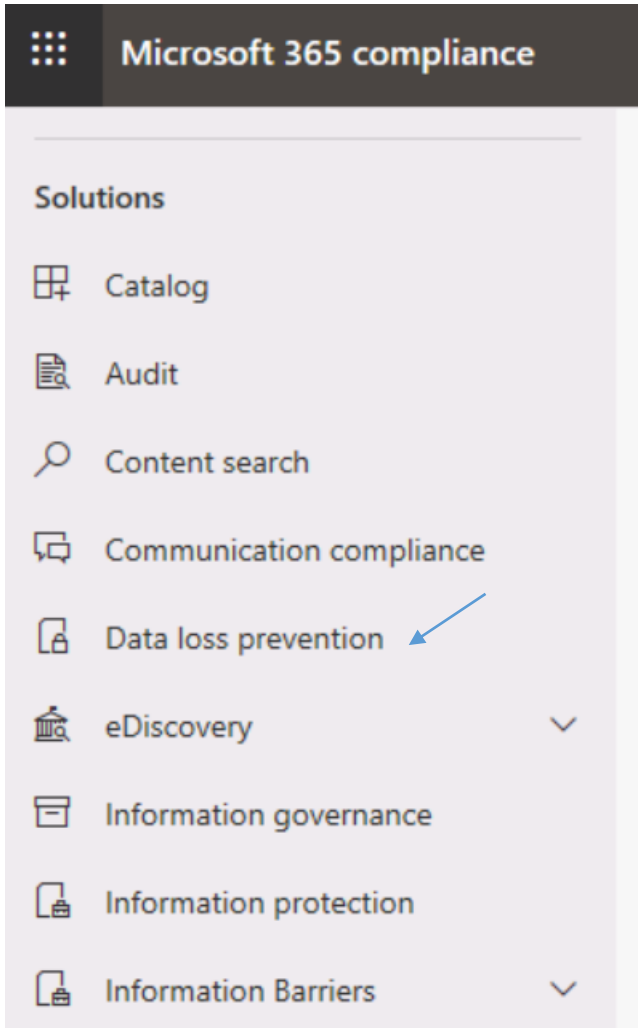
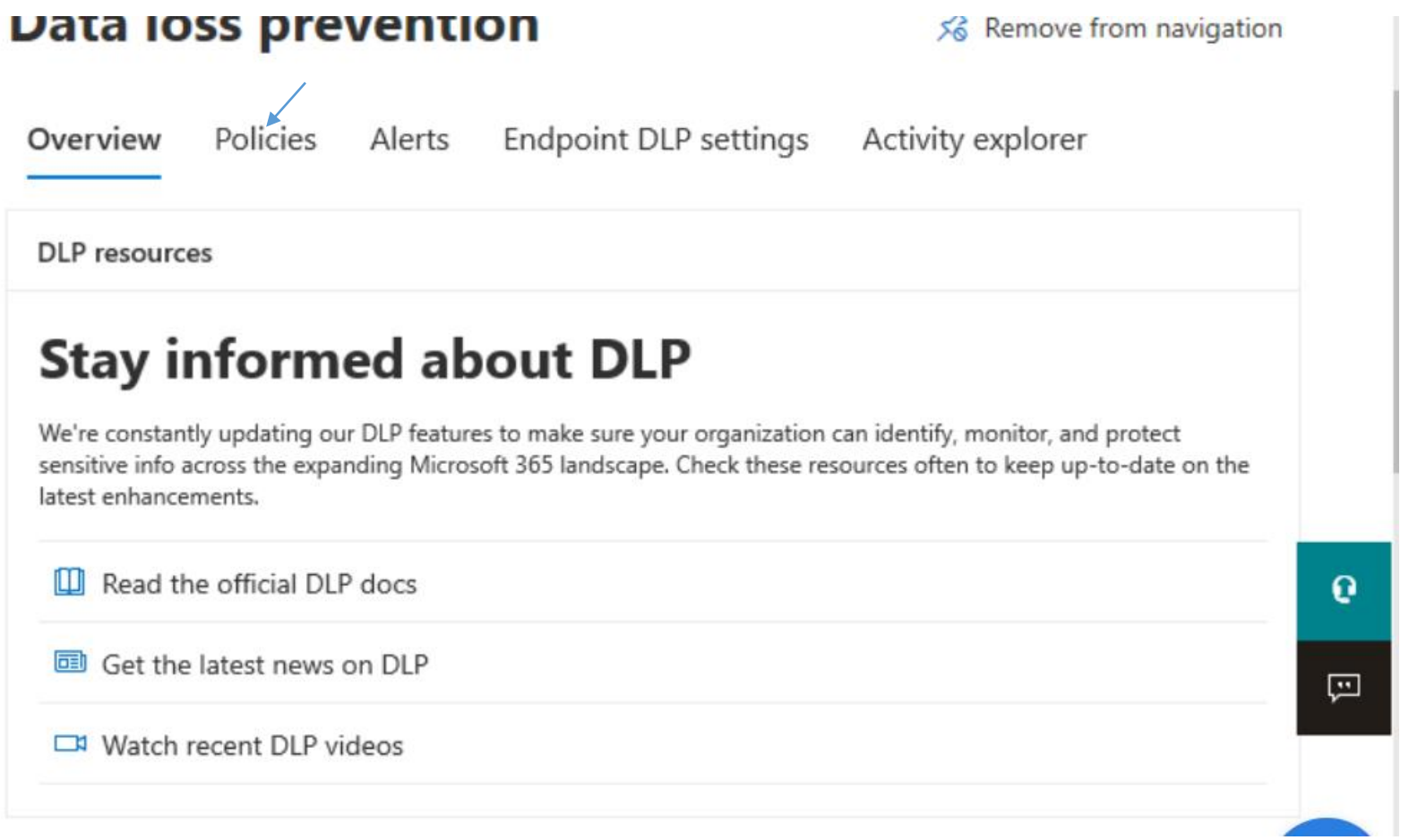
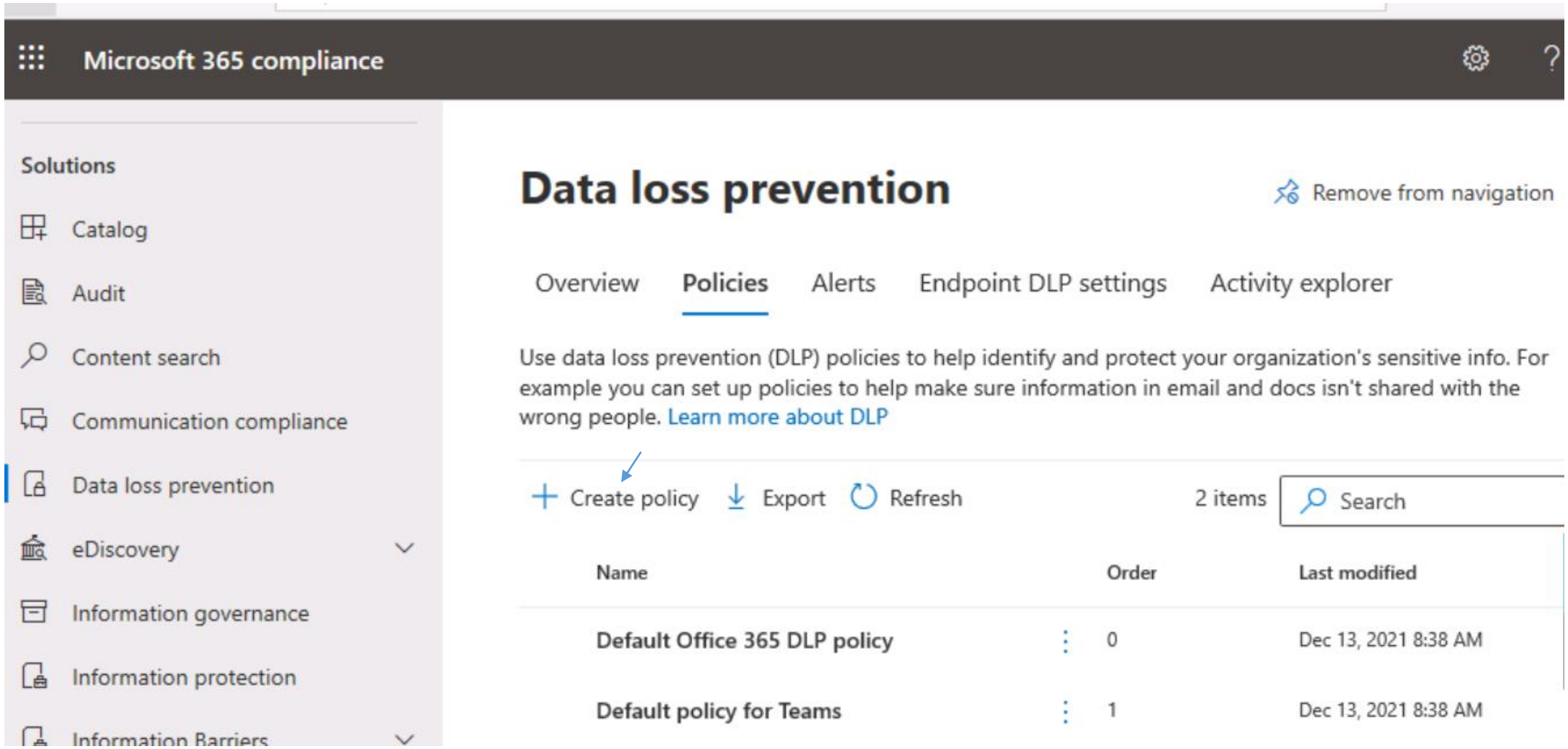
New data loss policy using template


https://admin.microsoft.com/Adminpc
Microsoft 365 admin center
Se
Setup
Reports
Health
Admin centers
Security
Compliance
Endpoint Manager
Azure Active Directo...
Exchange
Contoso
Compliance
Finish se
Now it's time to
With your Office


Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Information Barriers


Data loss prevention
Remove from navigation
Overview
Policies
Alerts
Endpoint DLP settings
Activity explorer
DLP resources
Stay informed about DLP
We're constantly updating our DLP features to make sure your organization can identify, monitor, and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.
Read the official DLP docs
Get the latest news on DLP
Watch recent DLP videos


Microsoft 365 compliance
Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Information governance
Information protection
Information Barriers
Data loss prevention
Remove from navigation
Overview
Policies
Alerts
Endpoint DLP settings
Activity explorer
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
Create policy
Export
Refresh
2 items
Search
Name
Order
Last modified
Default Office 365 DLP policy
0
Dec 13, 2021 8:38 AM
Default policy for Teams
1
Dec 13, 2021 8:38 AM

- Choose the information...
- Name your policy
- Locations to apply the pol...
- Policy settings
- Choose the information...
- Name your policy
- Locations to apply the pol...
- Policy settings
- Test or turn on the policy

Start with a template or create a custom policy

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

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Categories

- Financial
- Medical and health
- Privacy
- Custom

- U.K. Personal Information Online Code of Practice (PIOCP)
- U.S. Patriot Act Enhanced
- U.S. Patriot Act
- U.S. Personally Identifiable Information (PII) Data Enhanced
- U.S. Personally Identifiable Information (PII) Data

Helps detect the presence of information commonly considered to be personally identifiable information (PII) in the United States, including information like social security numbers or passport numbers.

Protect this information:

- U.S. Individual Taxpayer Identification Number (ITIN)
- U.S. Social Security Number (SSN)

Next

Choose the information t...
Name your policy
Locations to apply the pol...

Name your DLP policy

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

Name *

U.S. Personally Identifiable Information (PII) Data

Description

Helps detect the presence of information commonly considered to be personally identifiable information (PII) in the United States, including information like social security numbers or passport numbers.

Back | Next | Cancel

- Choose the information t...
- Name your policy
- **Locations to apply the p...**
- Policy settings
- Test or turn on the policy

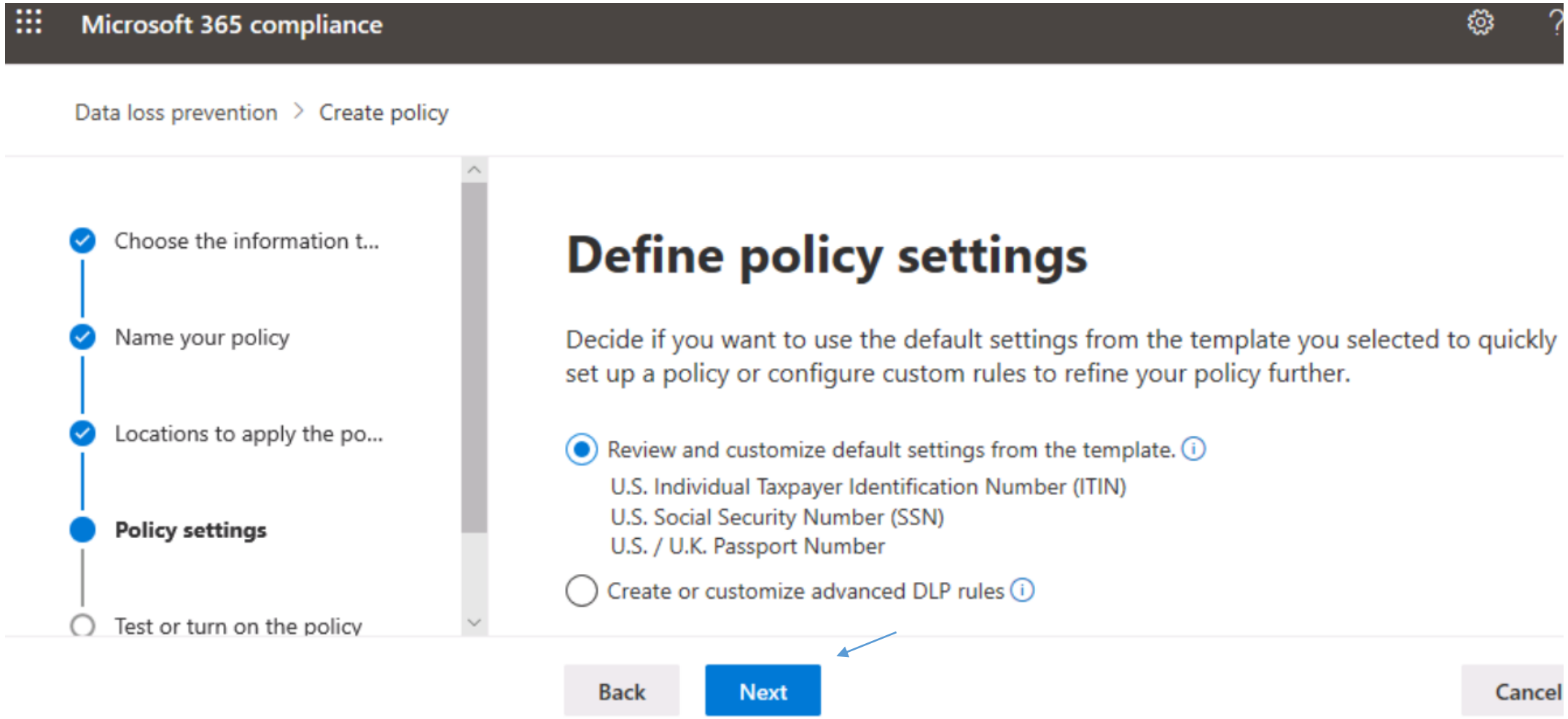
Choose locations to apply the policy

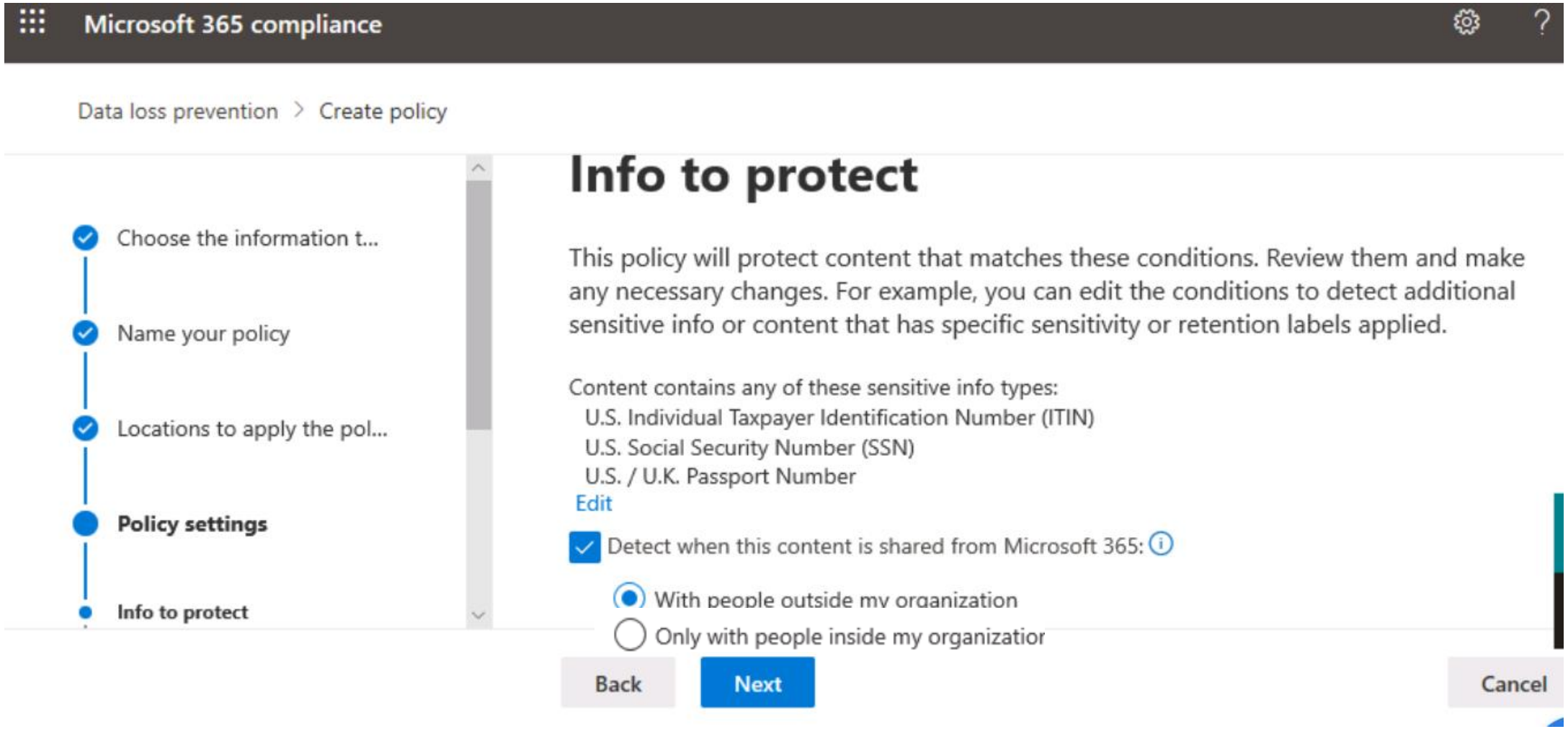
We'll apply the policy to data that's stored in the locations you choose.

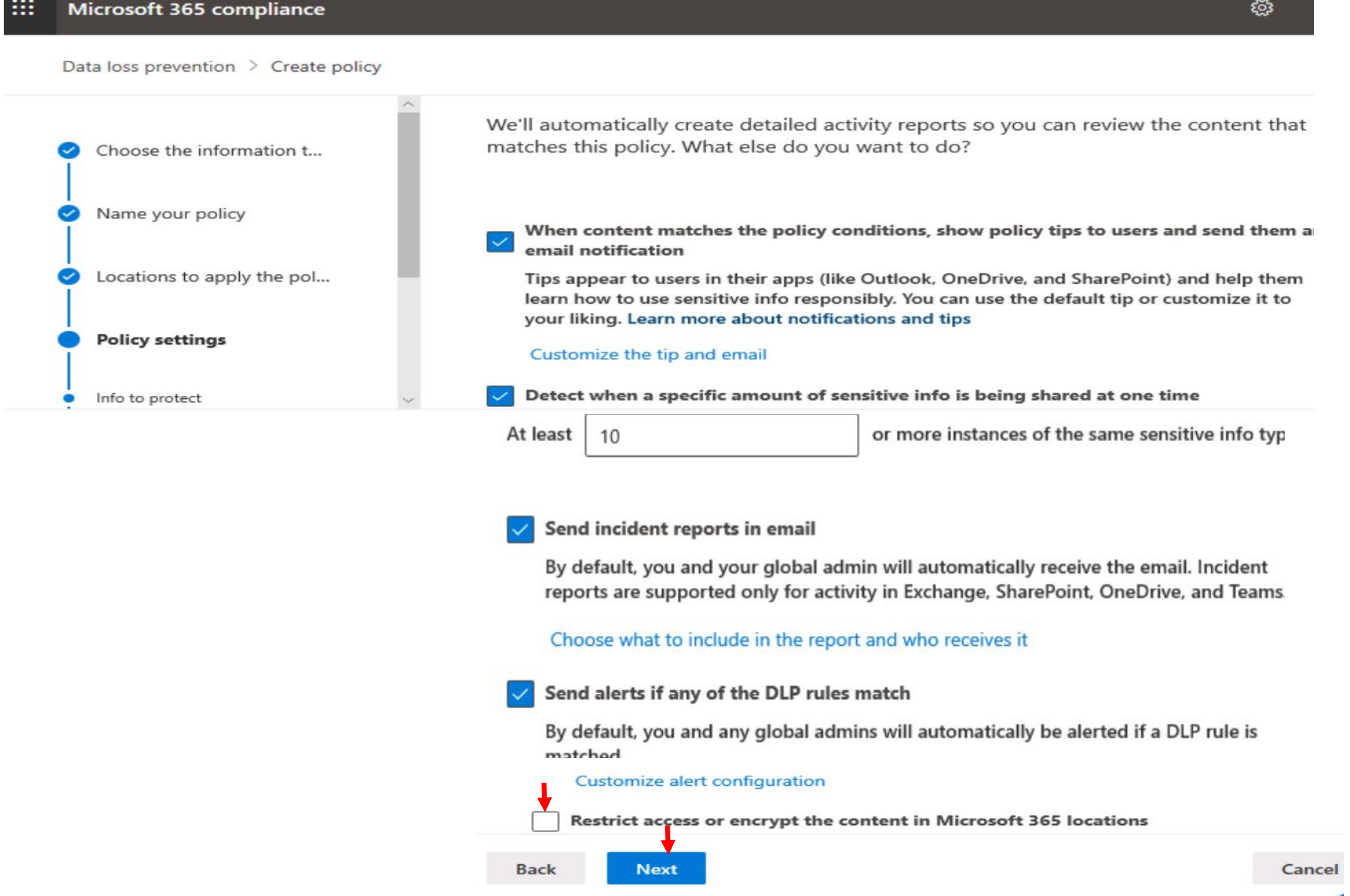
Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

Status	Location	Included	Excluded
On	Exchange email	All	None
Off	SharePoint sites	All Choose sites	None Exclude sites
Off	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
Off	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
Off	Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
Off	On-premises repositories	All Choose repositories	None Exclude repositories
Off	Power BI	All Choose workspaces	None Exclude workspaces

Back | Next | Cancel


Microsoft 365 compliance
Data loss prevention > Create policy
Choose the information t...
Name your policy
Locations to apply the po...
Policy settings
Test or turn on the policy
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.
U.S. Individual Taxpayer Identification Number (ITIN)
U.S. Social Security Number (SSN)
U.S. / U.K. Passport Number
Create or customize advanced DLP rules
Back
Next
Cancel


Microsoft 365 compliance
Data loss prevention > Create policy
Choose the information t...
Name your policy
Locations to apply the pol...
Policy settings
Info to protect
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:
U.S. Individual Taxpayer Identification Number (ITIN)
U.S. Social Security Number (SSN)
U.S. / U.K. Passport Number
Edit
Detect when this content is shared from Microsoft 365:
With people outside my organization
Only with people inside my organizatior
Back
Next
Cancel


Microsoft 365 compliance
Data loss prevention > Create policy
Choose the information t...
Name your policy
Locations to apply the pol...
Policy settings
Info to protect
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 a 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 typ
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
Send alerts if any of the DLP rules match
By default, you and any global admins will automatically be alerted if a DLP rule is matched
Customize alert configuration
Restrict access or encrypt the content in Microsoft 365 locations
Back
Next
Cancel

- Choose the information t...
- Name your policy
- Locations to apply the pol...
- **Policy settings**
- Info to protect

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 receiving email or accessing shared SharePoint, OneDrive, and Teams files.

By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

○ Block everyone. ⓘ

◉ Block only people outside your organization. ⓘ

☐ **Let people who see the tip override the policy**

☐ Require a business justification to override

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

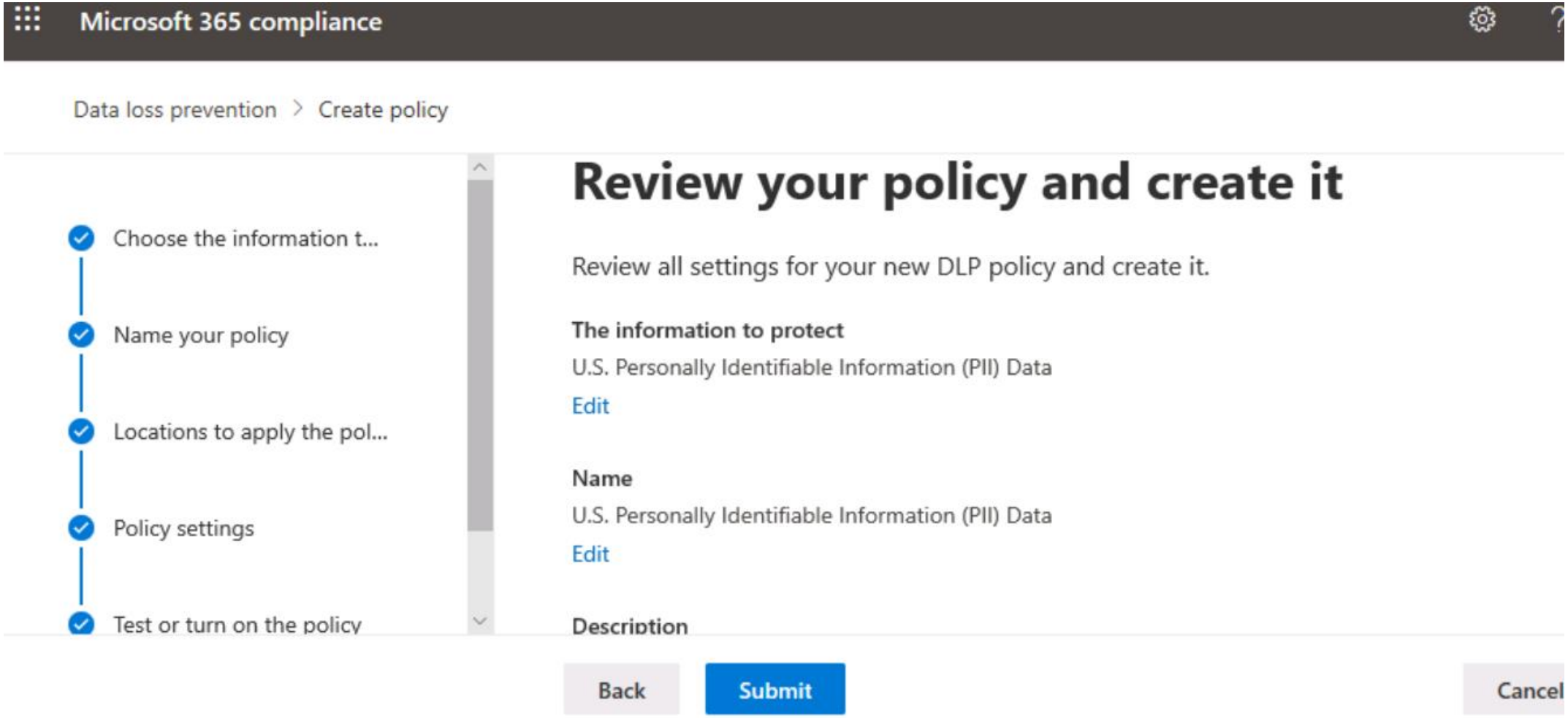
☐ **Restrict access or remove on-premises files**

◉ Block people from accessing files stored in on-premises repositories

○ Set permissions on the file (permissions will be inherited from the parent folder)

○ Move file from where it's stored to a quarantine folder

Back **Next**


Microsoft 365 compliance
Data loss prevention > Create policy
Choose the information t...
Name your policy
Locations to apply the pol...
Policy settings
Test or turn on the policy
Review your policy and create it
Review all settings for your new DLP policy and create it.
The information to protect
U.S. Personally Identifiable Information (PII) Data
Edit
Name
U.S. Personally Identifiable Information (PII) Data
Edit
Description
Back
Submit
Cancel

New policy created

Data loss prevention policy has been created.

Next steps

Monitor alerts to review policy matches. Learn about reviewing alerts

Related tasks

Further minimize risks by setting up one or more of these communication compliance policies to detect and act on inappropriate or sensitive messages in email and Teams.

Detect communications for inappropriate text

Detect communications for inappropriate images

Monitor communications for sensitive info

Monitor communications for conflicts of interest

Done

Data loss prevention

Remove from navigation

Overview | **Policies** | Alerts | Endpoint DLP settings | Activity explorer

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

+ Create policy | Export | Refresh

3 items | Search

Name	Order	Last modified	Status
Default Office 365 DLP policy	0	Feb 12, 2022 6:12 AM	On
Default policy for Teams	1	Feb 12, 2022 6:12 AM	On
U.S. Personally Identifiable Information (PII) Data	2	Mar 4, 2022 5:08 PM	Test without notifications