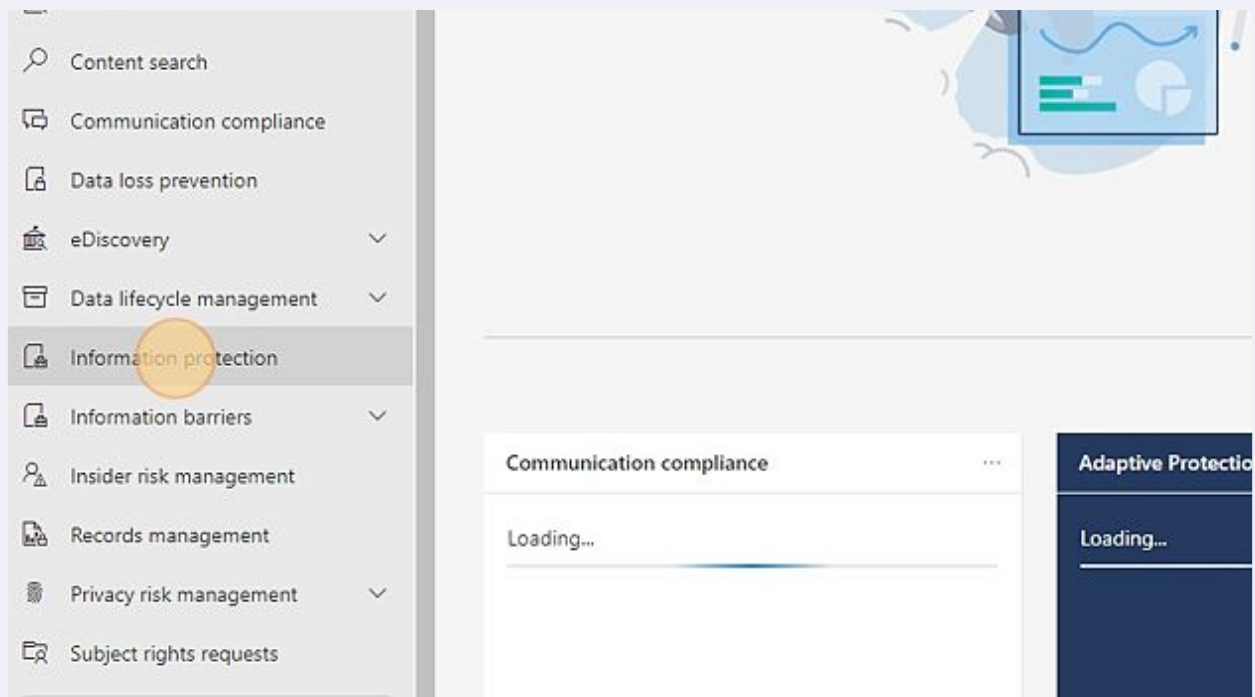


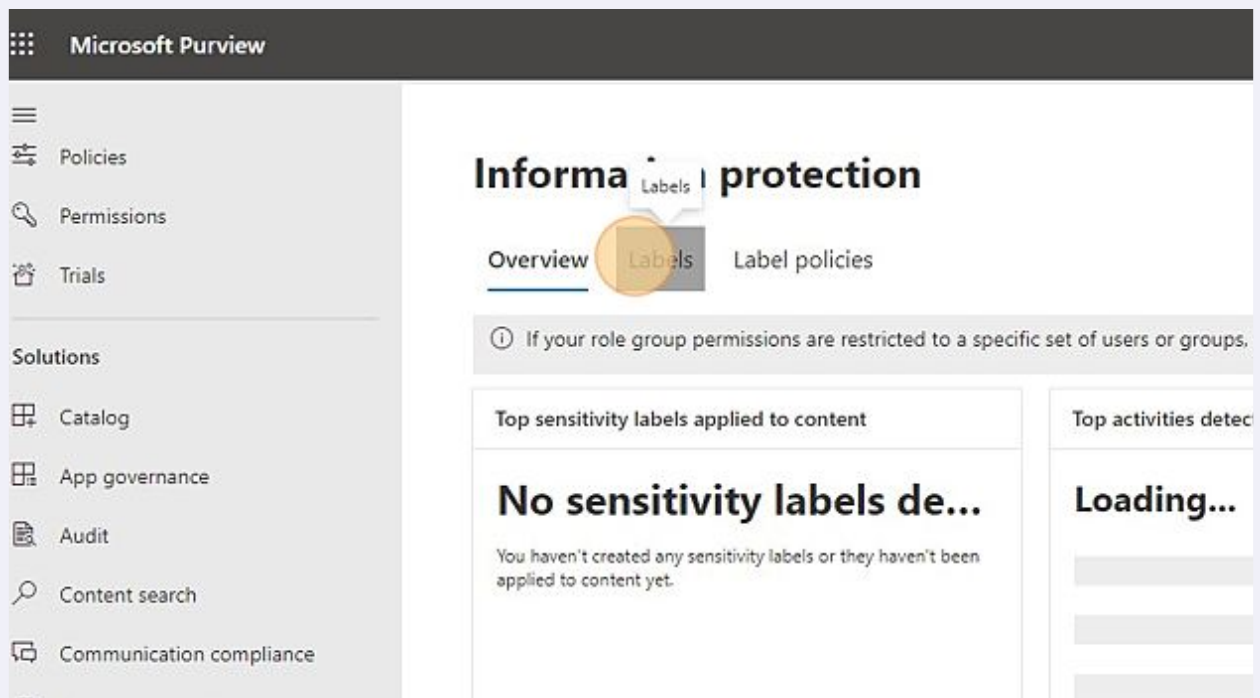
How to Create a General Sensitivity Label in Microsoft 365

1 Navigate to compliance.microsoft.com

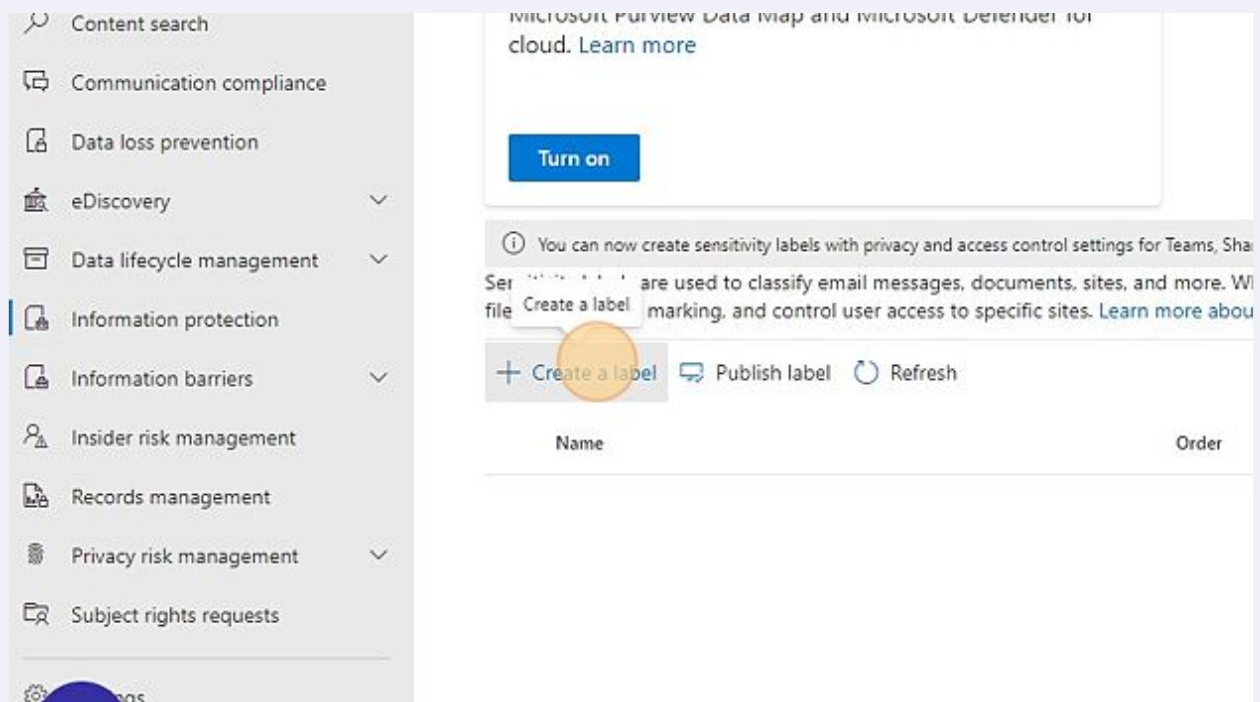
2 Click "Information protection"



3 Click "Labels"



4 Click "Create a label"



- 5 Type "General" into the "Name" field.

Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced. Labeled files will be protected wherever they go, whether they're saved locally or in the cloud.

Name * ⓘ
Enter a friendly name

Display name * ⓘ
Enter a display name. This is the name your users will see in the apps where it's used.

Description for users * ⓘ
Enter text that helps users understand this label's purpose

- 6 Enter this in the "Description for users" field

"This information includes internal business data which is NOT meant for public consumption. This information can be used by all employees and can be shared with authorized customers and business partners as needed."

General

Display name * ⓘ
General

Description for users * ⓘ
Enter text that helps users understand this label's purpose

Description for admins ⓘ
Enter a description that's helpful for admins who will manage this label

Label color

7

Click the "Description for admins" field.

"No visual marking, no encryption, no access restrictions"

The screenshot shows a form with two text input fields. The first field, labeled 'Description for users *', contains the text: 'This information includes internal business data which is NOT meant for public consumption with authorized customers and business partners as needed.' The second field, labeled 'Description for admins', is empty and has a yellow circle highlighting it. Below the fields is a 'Label color' section with a row of color swatches: black, gray, dark gray, purple, blue, green, yellow, orange, and red. A 'Next' button is at the bottom right.

8

Select "Gray" as the color.

The screenshot shows the same form as before, but now the 'Description for admins' field contains the text: 'Visual marking, no encryption, no access restrictions'. The 'Label color' section is highlighted with a yellow circle, and the 'Gray' color swatch is selected. The 'Next' button is at the bottom right.

9 Click "Next"

Description for users * ⓘ

This information includes internal business data which is NOT meant for p with authorized customers and business partners as needed.

Description for admins ⓘ

Visual marking, no encryption, no access restrictions

Label color

The color selected below is currently applied to the parent label. A want to use a different color, edit the parent label. [Learn more about](#)

Next

10 Select the scope for the label and click "Next"

Microsoft Purview

New sensitivity label

- ✓ Name & description
- **Scope**
- Items
- Groups & sites
- Finish

Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

☒ **Items**
Configure protection settings for labeled emails, Office files, and Power BI items. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

☐ **Groups & sites**
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.
ⓘ To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first [complete these steps](#) to enable the feature.

☐ **Schematized data assets (preview)**
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.
ⓘ To apply this label to schematized data assets, you must first turn on labeling for Microsoft Purview Data Map. You can do this from the Labels page. [Learn more about labeling for Microsoft Purview Data Map](#)

Back Next

11 No protections are required for the General label.

Microsoft Purview

New sensitivity label

- Name & description
- Scope
- Items**
- Groups & sites
- Finish

Choose protection settings for labeled items

Configure encryption and content marking settings to protect labeled items.

- ☐ **Apply or remove encryption**
Control who can access items that have this label applied.
- ☐ **Apply content marking**
Add custom headers, footers, and watermarks to items that have this label applied.

Back Next

12 Review settings and click "Create label"

Description
Visual marking, no encryption, no access restrictions
[Edit](#)

Scope
File, Email
[Edit](#)

Content marking
[Edit](#)

Auto-labeling for files and emails
[Edit](#)

Group settings
[Edit](#)

Site settings
[Edit](#)

Back Create label

13

Click "Don't create a policy yet
You can publish or auto-apply this label later."

ption



Your sensitivity label was created

Creating the label is just the first step in classifying and protecting content. To make this label available to users, auto-apply it to specific content and publish it to users' apps.

Next steps

- ☒ **Publish label to users' apps**
Create a label policy to make the label available in Office apps, SharePoint, Teams, and Microsoft 365 Groups. Once published, protect their content. [Learn more about publishing labels](#)
- ☐ **Don't create a policy yet**
You can publish or auto-apply this label later.

Recommended resources based on your settings

[Review prerequisites](#) to get the most out of your encryption settings

14

Click "Done"

✓ Scope

✓ Items

✓ Groups & sites

✓ Finish

Your sensitivity label was created

Creating the label is just the first step in classifying and protecting content. To make this label available to users, auto-apply it to specific content and publish it to users' apps.

Next steps

- ☐ **Publish label to users' apps**
Create a label policy to make the label available in Office apps, SharePoint, Teams, and Microsoft 365 Groups. Once published, protect their content. [Learn more about publishing labels](#)
- ☒ **Don't create a policy yet**
You can publish or auto-apply this label later.

Recommended resources based on your settings

[Review prerequisites](#) to get the most out of your encryption settings

