

Part 2 – Information Protection

Contents

Disclaimer.....	1
Target Audience	2
Document Scope	2
Out-of-Scope.....	2
Overview of Document	2
Use Case	3
Definitions.....	3
Notes.....	3
Pre-requisites	3
Create a Label	3
Publish your Label.....	7
Add a Label Policy	8
Testing Information Protection Policy	9
Appendix and Links	11

Disclaimer

This document is not meant to replace any official documentation, including those found at docs.microsoft.com. Those documents are continually updated and maintained by Microsoft Corporation. If there is a discrepancy between this document and what you find in the Compliance User Interface (UI) or inside of a reference in docs.microsoft.com, you should always defer to that official documentation and contact your Microsoft Account team as needed. Links to the docs.microsoft.com data will be referenced both in the document steps as well as in the appendix.

All of the following steps should be done with test data, and where possible, testing should be performed in a test environment. Testing should never be performed against production data.

Target Audience

The Information Protection section of this blog series is aimed at Security and Compliance officers who need to properly label data, encrypt it where needed.

Document Scope

This document is meant to guide an administrator who is “net new” to Microsoft E5 Compliance through:

- Create a label
- Publish a label
- Add a label
- Test sending a label

It is presumed that you already have a Sensitive Information Type that you want to use in your Information Protection policy. For the purposes of this document, I will use a copy of the U.S. Social Security Number (SSN) called “U.S. SSN – Numbers Only” that I created in Part 1 of this blog series.

Out-of-Scope

This document does not cover any other aspect of Microsoft E5 Compliance, including:

- Sensitive Information Types
- Exact Data Matches
- Data Protection Loss (DLP) for Exchange, OneDrive, Devices
- Microsoft Cloud App Security (MCAS)
- Records Management (retention and disposal)
- Advanced eDiscovery

It is presumed that you have a pre-existing of understanding of what Microsoft E5 Compliance does and how to navigate the User Interface (UI).

Overview of Document

1. Use Case
2. Definitions
3. Notes
4. Pre-requisites
5. Create a Label
6. Publish your Label
7. Add your Label Policy to a document

8. Test sending the label document to a non-approved user
9. Appendix and Links

Use Case

If you send data outside of the company, you want to be sure only the assigned Recipient can open and see the data.

Definitions

- Sensitivity Label – a metadata tag
- Publish Label – making the metadata tag available to your tenant

Notes

- I will be testing with a Word file named “1-MB-Test-SSN-1-MIP”. This stands for 1MB file with SSN information for Microsoft Information Protection (label) testing.
- Azure Purview is not relevant to this document, so you can ignore all mentions to it in the UI wizards.

Pre-requisites

- Create a Sensitive Information Type (SIT) in Part 1 of this blog series.
- Populate a OneDrive file with the related SIT information.

Create a Label

1. Go to **Information Protection -> Labels** and click **Create a label**.

 Create a label

2. Give the Label a **Name**, **Display Name**, **Description for users**, and an optional **Description for admins**. I am going to use “Confidential-SSNs” for all of these fields. When you have what you want, click **Next**.

Name * ⓘ
Confidential-SSNs

Display name * ⓘ
Confidential-SSNs

Description for users * ⓘ
Confidential-SSNs

Description for admins ⓘ
Confidential-SSNs

3. For the label scope, accept the defaults and click **Next**.

Files & emails
Configure encryption and control access to content. This label will automatically apply this label to content.
 ⓘ To set up auto-labeling for files in OneDrive, SharePoint, and Teams, click **Next**.

Groups & sites
Configure privacy, access control, and sharing options for groups and sites.
 ⓘ To apply sensitivity labels to Teams, SharePoint, and OneDrive, click **Next**.

Azure Purview assets (preview)
Apply label to assets in Azure Purview.

4. You do not have to enable encryption or manage the content of the files. I will enable both. Click **Next** when you are ready.

Encrypt files and emails
Control who can access files and emails that have this label applied.

Mark the content of files
Add custom headers, footers, and watermarks to files and emails that have this label applied.

5. For encryption, accept the defaults for encryption and access as seen below.

Remove encryption if the file or email is encrypted

Configure encryption settings

i Turning on encryption impacts Office files (Word, PowerPoint) when the files are opened or saved, and some SharePoint a

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically

User access to content expires ⓘ

Never

Allow offline access ⓘ

Always

6. When it comes to permissions, add the test users you want to use. I am using my accounts of admin and Pradeep. When you are satisfied, click **Next**.

Assign permissions to specific users and groups * ⓘ

[Assign permissions](#)

Users and groups

PradeepG@[redacted].com

admin@[redacted].com

7. Enable Content marking and add a watermark, header and/or footer. For content marking, I will only be doing a watermark. I will make my watermark as large as possible to make it simple to see the watermark. Below is an example of what you can enter. Enter what makes the most sense for your testing and click **Save**. Then click **Next**.

Watermark text *

Social Security Numbers

Font size

52

Font color

Red

Text layout

Diagonal

8. I will not be performing Auto-labeling in this document. This is to avoid any excess performance overhead and allow for a precise testing. Click **Next**.
9. We are not going to protect any groups or sites in this document, so you can click **Next**.
- 10.** For **Azure Purview assets (preview)**, accept the default of disabled, and click **Next**.
11. Review your label and click **Create Label**. Then click **Done**.

Review your settings and finish

Name

Confidential-SSNs

[Edit](#)

Display name

Confidential-SSNs

[Edit](#)

Description for users

Confidential-SSNs

[Edit](#)

Description

Confidential-SSNs

[Edit](#)

Scope

File,Email,PurviewAssets

[Edit](#)


Encryption

Encryption

[Edit](#)

Publish your Label

1. Go to **Information Protection -> Label Policies** and click **Publish label**.

 Publish label


2. Choose your new label. Mine is “Confidential-SSNs”. Click **Next**.

Sensitivity labels to publish


Confidential-SSNs

[Edit](#)

3. For users and Groups, I will accept the default of “All” and click **Next**.

Location	Included
 Users and groups	All Choose user or group

4. I will enable the top to options around requiring a user to have justification to change a classification and requiring them to apply a label to their documents. When you are satisfied, click **Next**.

- Users must provide a justification to remove a label or lower its classification**
Users will need to provide a justification before removing a label or replacing it with a on changes and justification text.
- Require users to apply a label to their emails and documents**
Users will be required to apply labels before they can save documents, send emails, and c
 Support and behavior for this setting varies across apps and platforms. [Learn more](#)
- Provide users with a link to a custom help page**
If you created a website dedicated to helping users understand how to use labels in your

5. I will not be applying this label by default to documents. Again, I want to be very specific in my testing and avoid “test creep”. I will accept the default of “None” and click **Next**.

Apply this default label to documents

None

6. Again, I will not be applying this label by default to emails. I will accept the default of “None” but require them to apply the label to emails. Click **Next**.

Apply this default label to emails

None

Require users to apply a label to their emails

7. For Power BI labeling, accept the default and click **Next**.
8. I will use the same name and description of “Confidential-SSNs” that I applied to my label. This will simplify any troubleshooting between the label and policy. Click **Next** when you are ready.
9. Finally, review your published label, and click **Submit**. Then click **Done**.

Review and finish

Name

Confidential-SSNs

[Edit](#)

Description

Confidential-SSNs

[Edit](#)

Publish these labels

Confidential-SSNs

[Edit](#)

Publish to users and groups

All

[Edit](#)

Policy settings

Label is mandatory for: documents, emails

Users must provide justification to remove a label or lower its classification


[Edit](#)

10. With your label created and published, you can

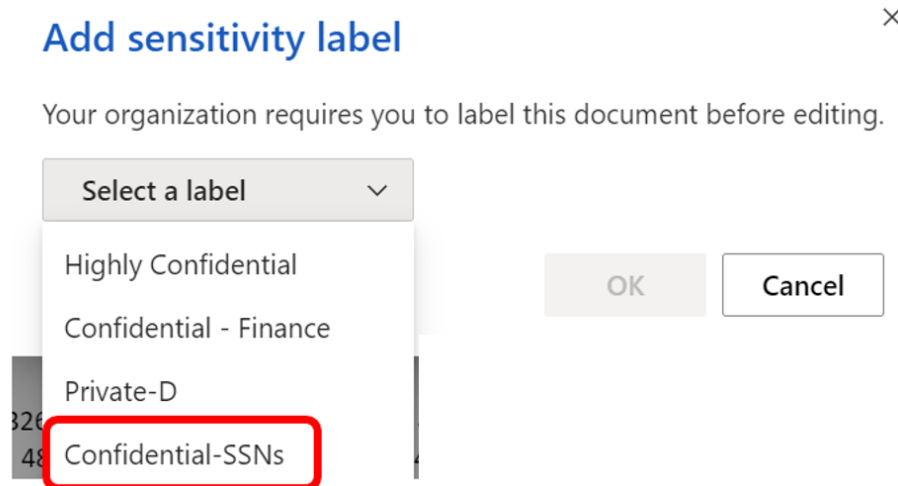
Add a Label Policy

1. Go to a file in your test account’s OneDrive. I will be using a Word file named “1-MB-Test-SSN-1-MIP”.

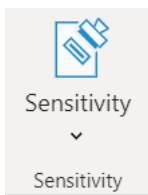
2. You will be prompted to add a label once your label is published to your tenant. You will not be able to modify your document until you add a label.

 **Add sensitivity label** Your organization requires you to label this document before editing.

3. Click **Select Label** on the right and select you the label you want and click **OK**. I will be choosing the Confidential-SSNs label created earlier.



4. If the prompt mentioned above does not appear, you can add a label in by going to the Word Tool bar, on the right, click on **Sensitivity**.



5. Select your label you create earlier. Remember, if you are not seeing your label, you might have to wait longer to have it appear.
6. Once you have added your label you are not ready to move to the testing of Information Protection in the next section.

Testing Information Protection Policy

Now we will email this label filed to a non-approved user.

1. Open your O365 email client.

2. Create an email and attach a the file to which you have applied your Information Protection label. want. I am emailing an external 'gmail' address who is not approved to view my test file. When you are ready, click **Send**.
3. Go to your recipient test email. I am using an external 'gmail' address for my testing. In the email click on **Read the message**.

MOD Administrator ([admin@\[REDACTED\].com](mailto:admin@[REDACTED].com)) has sent you a protected message.



[Read the message](#)

[Learn about messages protected by Office 365 Message Encryption.](#)

4. You will be asked to sign in with your credentials or with a One-time passcode. I will be using the passcode option.

Sign in to view the message



[Sign in with a One-time passcode](#)

5. Once you've clicked the **Sign in with a One-time passcode**, you will be sent an email with the code.

We sent a one-time passcode to sam.legal.compliance@gmail.com.

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode

This is a private computer. Keep me signed in for 12 hours.

6. Enter your code and you should see the following message stating **You don't have permission to view this message**.

You don't have permission to view this message

This message is protected and you don't have permission to view it.

7. You have now completed your initial testing of your Information Protection. You are now ready move to the next part of this blog.

Appendix and Links

- [Learn about sensitivity labels - Microsoft 365 Compliance | Microsoft Docs](#)
- [Use sensitivity labels with Microsoft Teams, Microsoft 365 groups, and SharePoint sites - Microsoft 365 Compliance | Microsoft Docs](#)
- [Enable archive mailboxes in the Security & Compliance Center - Microsoft 365 Compliance | Microsoft Docs](#)
- [Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs](#)
- [Use sensitivity labels with Microsoft Teams, Microsoft 365 groups, and SharePoint sites - Microsoft 365 Compliance | Microsoft Docs](#)
- [Automatically apply a sensitivity label to content in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs](#)
- [Use sensitivity labels with Microsoft Teams, Microsoft 365 groups, and SharePoint sites - Microsoft 365 Compliance | Microsoft Docs](#)
- [Automatically apply sensitivity labels to your data - Azure Purview | Microsoft Docs](#)
- [Manage sensitivity labels in Office apps - Microsoft 365 Compliance | Microsoft Docs](#)
- [Mandatory label policy in Power BI - Power BI | Microsoft Docs](#)
- [Automatically apply a sensitivity label to content in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs](#)