AZURE INFORMATION PROTECTION
QUICK GUIDE

Table of Contents

What is Azure Information Protection?....1

Using Office apps to classify and protect your documents 2

Set custom permissions for a document in office Apps 3

Using File Explorer (AIP AGENT) to classify and protect files 4

Track and revoke your documents 6

Track and revoke documents using the office app (Word, Excel, PowerPoint, and Outlook) 6

Track and revoke non-office file(s) (PDF/Images) using the AIP Agent 7

View and use files that have been protected by AIP....8

Safely share a file outside the organization....9

NEW Automatic detection of sensitive information....10

What is Azure Information Protection?

Azure Information Protection (AIP) is a solution that empowers its users to label and protect documents. This is done through labels and the two that our caregivers will see by default are Public – Unprotected and Internal – Protected. There is also an option to set custom permissions.

- **Public – Unprotected**: This does not apply any protection and the documents/emails will be accessible by anybody.

- **Internal – Protected**: This should be used to restrict access to anyone that has a PeaceHealth email account. This should be used for protecting document with sensitive enough information that shouldn't be viewed outside our organization.

- **Custom Permissions**: If neither of the two default labels are applicable to your situation you can use custom permissions. How this is done will be explained in the following documentation.

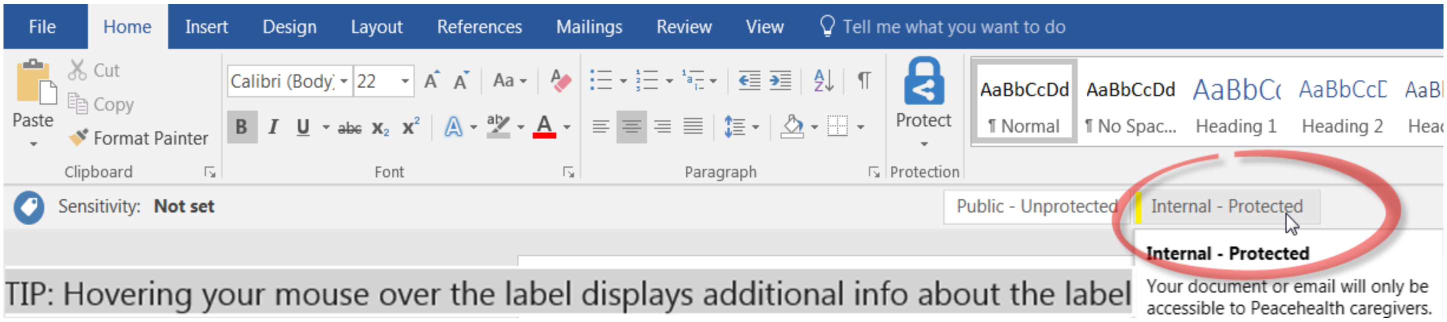
The easiest way to classify and protect your documents and emails is when you are creating or editing them from within your Office desktop apps: **Word**, **Excel and PowerPoint**.

However, you can also classify and protect files by using **File Explorer** (with the **AIP agent installed)**. This method supports additional file types (besides Office docs) to include PDF files, text and image files. It is also a convenient way to classify and protect multiple files at once.

Using Office apps to classify and protect your documents

1. Using the Azure Information Protection bar, **select** the appropriate label for your document.

*For example, the following picture shows that the document hasn't yet been labeled because the **Sensitivity** shows **Not set**. To set a label, such as "Internal", click **Internal**.*



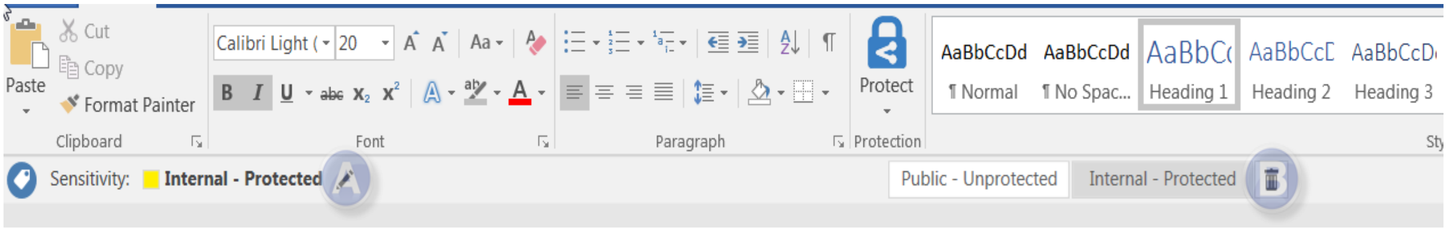
Sensitivity: **Not set**

TIP: Hovering your mouse over the label displays additional info about the label

Internal - Protected
Your document or email will only be accessible to Peacehealth caregivers.

2. If a label is already applied to the document and you want to change it:

A. **click** on **edit label** icon
B. **click** on **delete label** icon and choose a different label

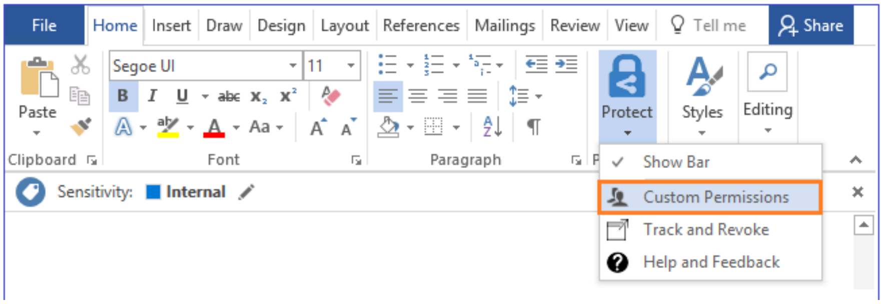


Sensitivity: **Internal - Protected**

Set custom permissions for a document in office Apps

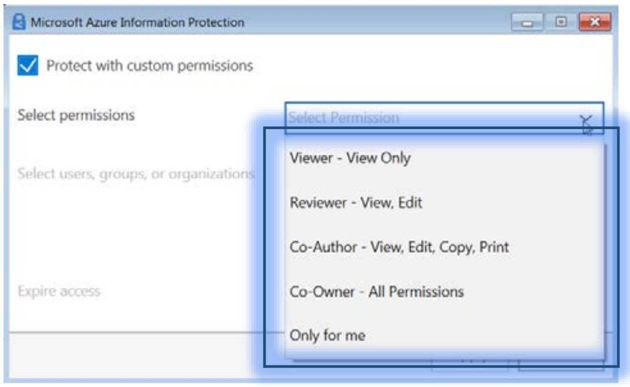
You can specify your own protection settings for documents rather than use the labels provided.

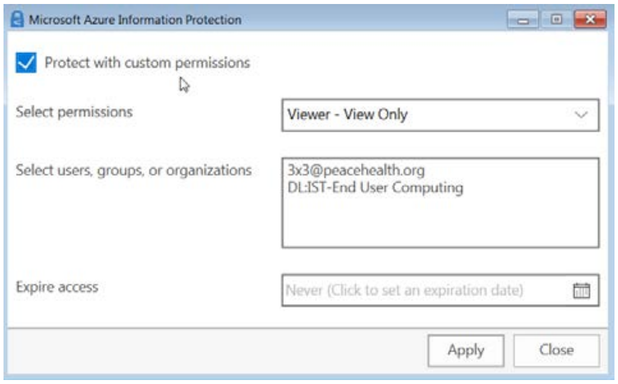
1. On the **Home** tab, in the **Protection** group, click **Protect** > **Custom Permissions**:



**Note that any custom permissions that you specify <u>replace</u> rather than supplement protection settings of a selected label.*

2. In the **Microsoft Azure Information Protection** dialog box, specify the following:


Microsoft Azure Information Protection
Protect with custom permissions
Select permissions
Select Permission
Select users, groups, or organizations
Expire access
Viewer - View Only
Reviewer - View, Edit
Co-Author - View, Edit, Copy, Print
Co-Owner - All Permissions
Only for me



☑ Protect with custom permissions

Select permissions: Viewer - View Only

Select users, groups, or organizations: 3x3@peacehealth.org
DL:IST-End User Computing

Expire access: Never (Click to set an expiration date)

Note: You can't set custom permissions on an email at this time

- **Protect with custom permissions**: Make sure that this is selected so that you can specify and apply your custom permissions. Clear this option to remove any custom permissions.
- **Select permissions**: Select the level of access that you want specified people to have.
- **Select users, groups, or organizations**: Specify the people who should have the permissions you selected for your file or files. Type their full email address, distribution list, or a domain name from the organization for all users in that organization.
- **Expire access**: Select this option only for time-sensitive files so that the people you specified will not be able to open your selected file or files after a date that you specify. You will still be able to open the original file, but after midnight (your current time zone), on the day that you select, no one but you will be able to open the file.

3. Click **Apply** and wait for the **Custom permissions applied** message. Then click **Close**.

Using File Explorer (AIP AGENT) to classify and protect files

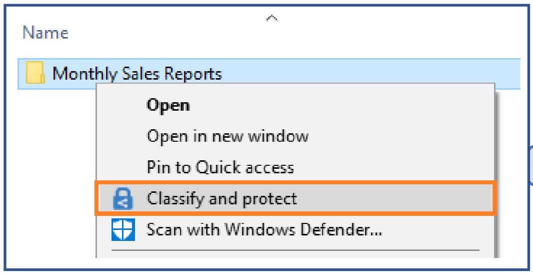
When you use File Explorer, you can quickly classify and protect a single file, multiple files, or all files in a folder.

When you select a folder, all the files in it and any subfolders it has are automatically selected for the classification and protection options that you set.

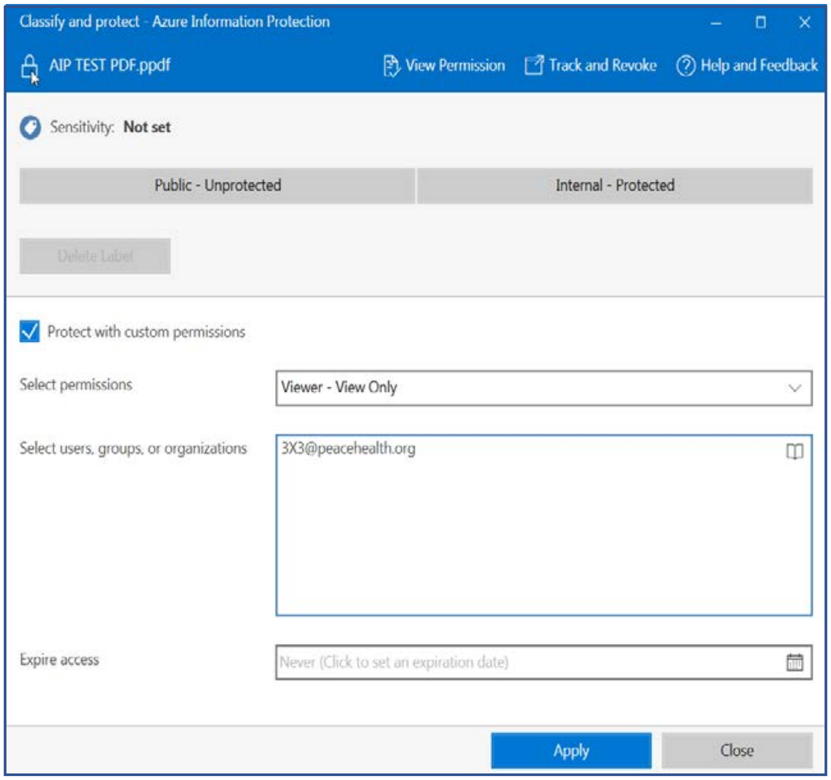
However, new files that you create in that folder or subfolders are not automatically configured with those options **as the folder itself is not protected, only the files**. Some files are automatically excluded from classification and protection, because changing them might stop your PC from running. Examples include executable files and your Windows folder.

Classify and protect file(s) by using File Explorer

1. Select your file, multiple files, or a folder.



2. Right-click, and select **Classify and protect**. (Doing so will bring up the AIP agent.)



Sensitivity: Not set

☑ Protect with custom permissions

Select permissions: Viewer - View Only

Select users, groups, or organizations: 3X3@peacehealth.org

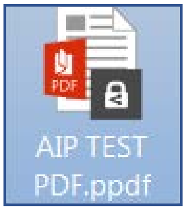
Expire access: Never (Click to set an expiration date)

AIP AGENT

3. In the **Classify and protect - Azure Information Protection** dialog box, use the labels as you would in an Office application, which sets the classification and protection as defined by your administrator. You also have the option to set **custom permissions** in the same way shown in the previous section.

The selected file or files are now classified and protected, according to your selections. In some cases (non-office files), the original file is replaced with a new file that has the Azure Information Protection lock icon.

If you change your mind about the classification and protection, or later need to modify your settings, simply repeat this process with your new settings.



The classification and protection that you specified stays with the file, even if you email or save it to another location. If you protected the file, you can track how people are using it and if necessary, revoke access to it.

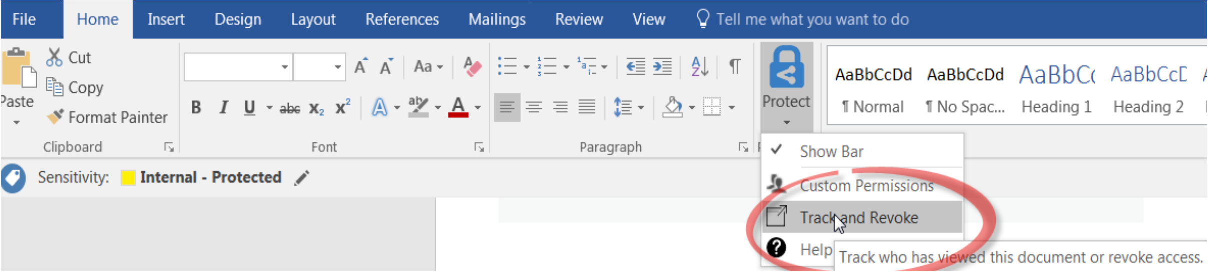
Track and revoke your documents

After you have protected your documents by using Azure Information Protection, you can track how people are using these documents.

If necessary, you can also revoke access to them if people should no longer be able to read them.

Track and revoke documents using the office app (Word, Excel, PowerPoint, and Outlook):

1. On the **Home** tab, in the **Protection** group, click **Protect**.

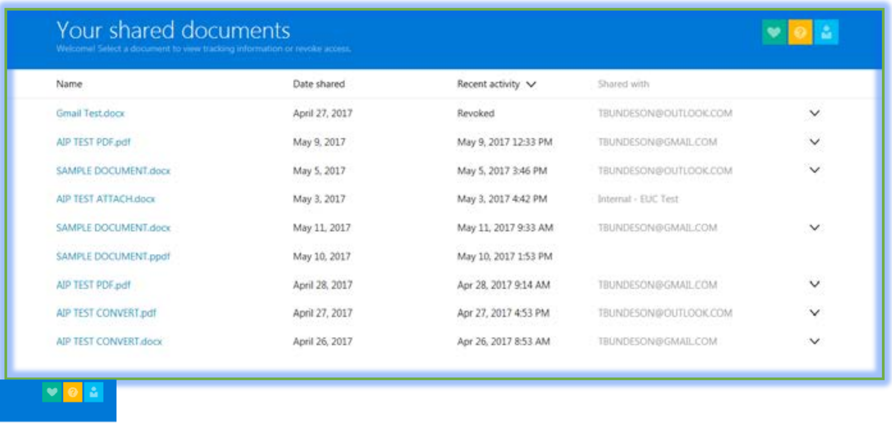


Sensitivity: Internal - Protected

Track who has viewed this document or revoke access.

2. Clicking on **Track and Revoke** will take you to the **document tracking site.**
3. **Sign in** to track your documents.

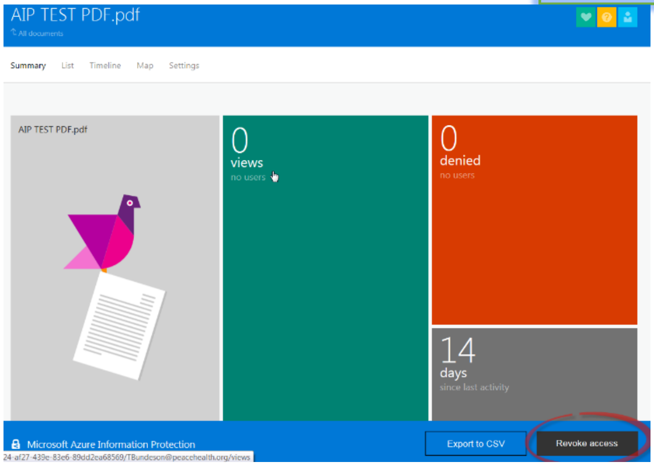
When you access this site, you can then see who tried to open the files that you protected and whether they were successful (they were successfully authenticated) or not. You will also see each time they tried to access the document, and their location at the time.



Your shared documents

Welcome! Select a document to view tracking information or revoke access.

Name	Date shared	Recent activity	Shared with
Gmail Test.docx	April 27, 2017	Revoked	TBUNDESON@OUTLOOK.COM
AIP TEST PDF.pdf	May 9, 2017	May 9, 2017 12:33 PM	TBUNDESON@GMAIL.COM
SAMPLE DOCUMENT.docx	May 5, 2017	May 5, 2017 3:46 PM	TBUNDESON@OUTLOOK.COM
AIP TEST ATTACH.docx	May 3, 2017	May 3, 2017 4:42 PM	Internal - EUC Test
SAMPLE DOCUMENT.docx	May 11, 2017	May 11, 2017 9:33 AM	TBUNDESON@GMAIL.COM
SAMPLE DOCUMENT.ppdf	May 10, 2017	May 10, 2017 1:53 PM	
AIP TEST PDF.pdf	April 28, 2017	Apr 28, 2017 9:14 AM	TBUNDESON@GMAIL.COM
AIP TEST CONVERT.pdf	April 27, 2017	Apr 27, 2017 4:53 PM	TBUNDESON@OUTLOOK.COM
AIP TEST CONVERT.docx	April 26, 2017	Apr 26, 2017 8:53 AM	TBUNDESON@GMAIL.COM

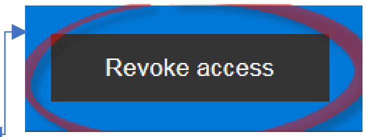


24-af27-439e-83e6-89dd2ea68569/TBundeson@peacehealth.org/views

4. To **stop sharing a document**

Click **Revoke access**

When you revoke a document, it doesn't delete the document that you shared, but authorized users will NO longer be able to open it

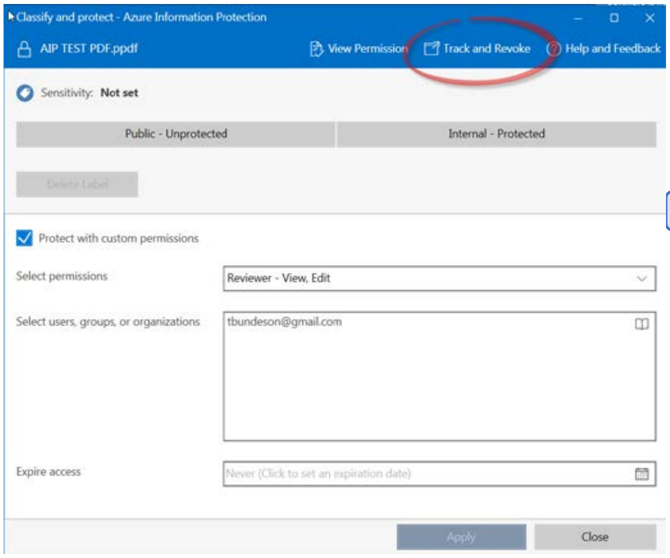


***Note** that you can click on the menus at the top of the page to view a **list, timelines, map** (location). **Under settings**; choose whether you want to be notified via email when someone opens or tries to open and gets subsequent denial for the protected document. **Default is no email notification**.*

Track and revoke non-office file(s) (PDF/Images) using the AIP Agent

1. Click to **open** your document.

2. Click **Track and Revoke.**



Sensitivity: **Not set**

☑ Protect with custom permissions

Select permissions: Reviewer - View, Edit

Select users, groups, or organizations: tbundeson@gmail.com

Expire access: Never (Click to set an expiration date)

3. **Sign in** and follow previous instructions.

View and use files that have been protected by AIP

You can often view a protected file by simply opening it. For example, you might double-click an attachment in an email message or double-click a file from File Explorer, or you might click a link to a file.

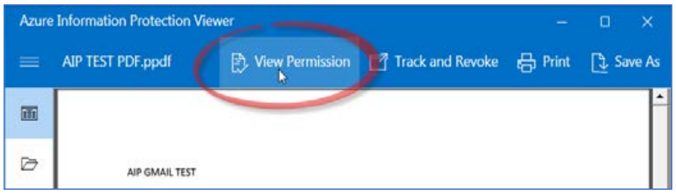
There are certain requirements before you’re able to open protected documents:

- Before you can view the protected file, the Azure Rights Management service that was used to protect the file must first confirm that you are **authorized** to view the file.
- Must have OfficePro Plus 2010 or above to view protected **office documents** (Word, Excel, Powerpoint).

- To open protected **non-office files** (PDF, image files), clicking on the document will open the AIP viewer that comes bundled with the AIP agent (installed on PH machines)

*If you are prompted to select an app, select **Azure Information Protection***

- You can check your permissions for the file by clicking **Permissions**. From the **Permissions** dialog box, you can also identify the file owner to contact if you want to request a new version of the file with additional permissions.



Safely share a file outside the organization

If you regularly share files with people outside our PH organization, your administrator might configure a label for you that sets protection such that these external recipients can read it.

Alternatively, you can use your Office app or **File Explorer** to set custom permissions for a file before you share it.

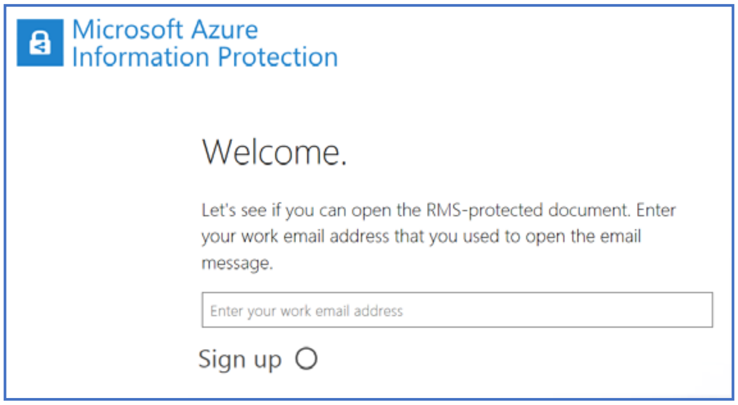
If you set your own custom permissions and the file is already protected for internal use, first make a copy of it to retain the original permissions. Then use the copy to set the custom permissions.

When the file is protected with your custom permissions, use your standard sharing mechanism to share the file. If this is the first time that these people that you are sharing with have received a protected file, they might need instructions to view it. You can copy and paste the following message:

I've protected this file with Microsoft Azure Information Protection.

For first time use, see these instructions.

The link will take them to the MS Azure Information Protection site where their work email address is validated by Microsoft. Personal email addresses are not allowed at the time of this writing. However, popular email addresses such as Gmail and Hotmail will be validated in the near future per Microsoft.

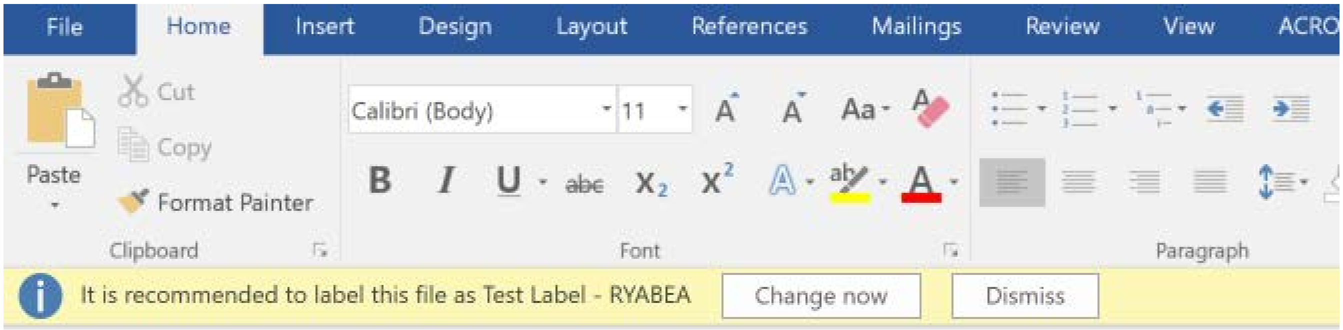

Microsoft Azure Information Protection

Welcome.

Let's see if you can open the RMS-protected document. Enter your work email address that you used to open the email message.

Automatic detection of sensitive information

When sensitive information (i.e. SSN, credit card #, etc.) is detected in your document(s) you will be prompted with a recommendation to protect you documents.



It is recommended to label this file as Test Label - RYABEA

*Note: Instead of "Test Label – RYABEA" it will show "Internal – Protected"

You will have the option to apply the recommended label with the Change now button or you can click Dismiss if it has incorrectly detected sensitive information.