What is Azure Information Protection (AIP)?

Azure Information Protection (AIP) is a cloud-based solution that enables organizations to classify and protect documents and emails by applying labels.

Azure Information Protection (AIP) will be deployed automatically if workstation is connected to the Government network (MAGNET). If installed correctly you will see the sensitivity button as shown below.

If workstation is not connected to the MAGNET, one can install AIP client through the below link;

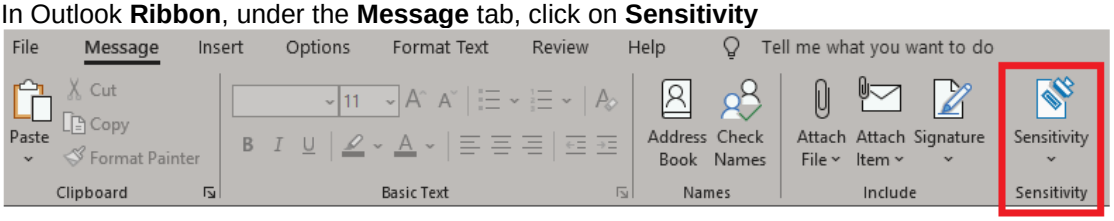
https://www.microsoft.com/en-us/download/details.aspx?id=53018

01. Composing a new Secure Email

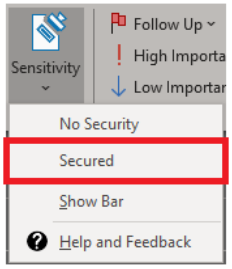
1. Open **Microsoft Outlook**

2. Click on **New Email**

3. In Outlook **Ribbon**, under the **Message** tab, click on **Sensitivity**

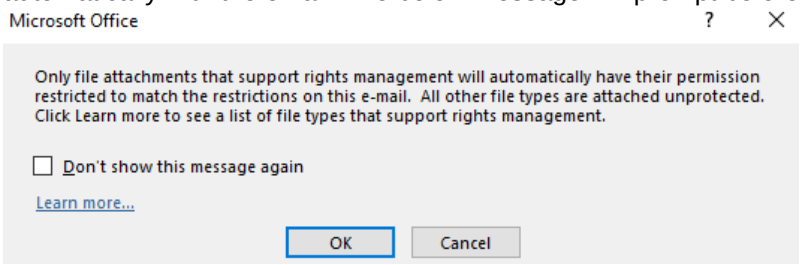


4. Select the **Secured** option



5. Once the **Secured** option is selected, the below message will be displayed at the top of the email

6. Attachments which support rights management, will have their permissions restricted automatically with the email. The below message will prompt before sending the email,

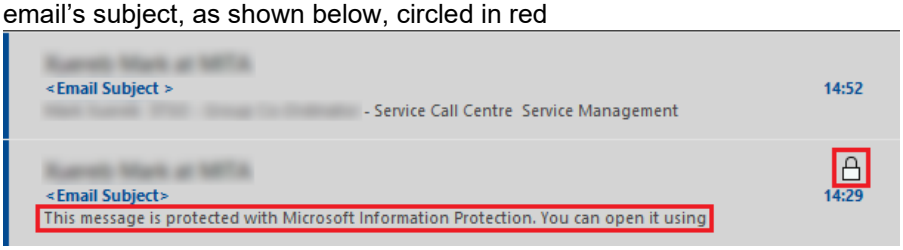


7. Click **OK** to continue with sending the Email

NOTE: New recipients can only be added by the owner of the email thread.

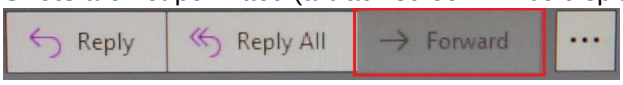
02. Reading a Secure Email from a Government Mailbox

1. A secure email can be identified as it will have a **lock** symbol and a **message** under the email's subject, as shown below, circled in red



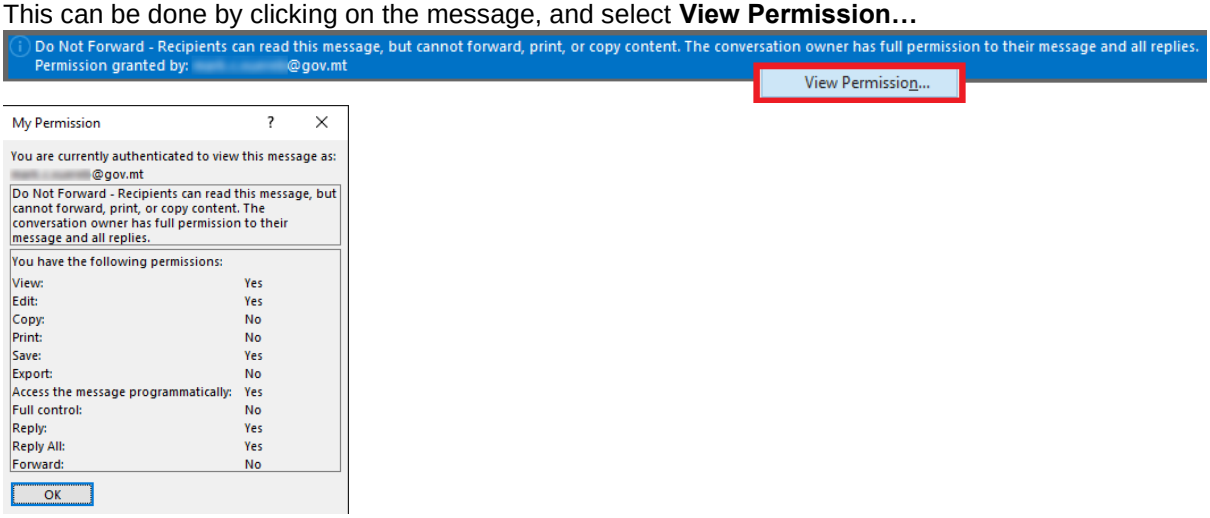
14:52
- Service Call Centre Service Management
<Email Subject>
14:29
This message is protected with Microsoft Information Protection. You can open it using

2. Secure email cannot be forwarded, the **Forward** button will be disabled, and any **Screen Shots** are not permitted (a black screen will be displayed in the screen shot)



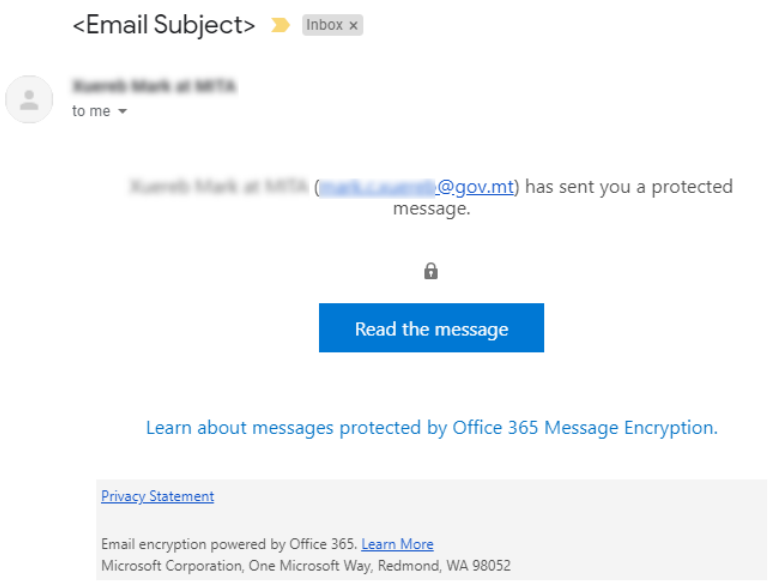
3. The below message will also be displayed in the email, where recipients can see their permissions on that specific email.

   This can be done by clicking on the message, and select **View Permission…**

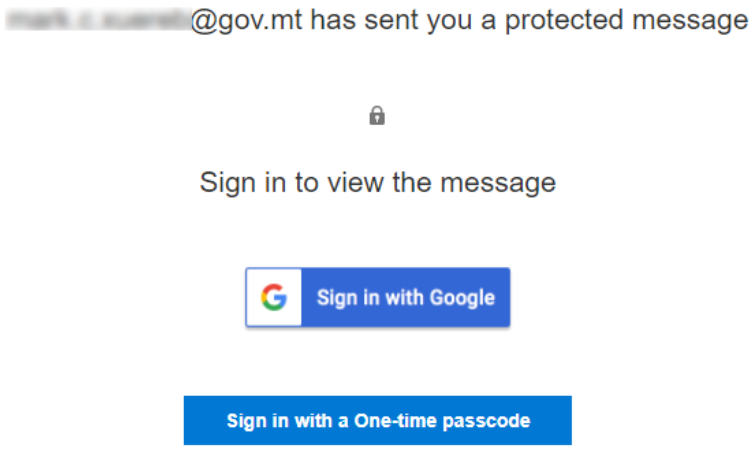


03. Reading a Secure Email from a 3rd Party account (i.e. Gmail)

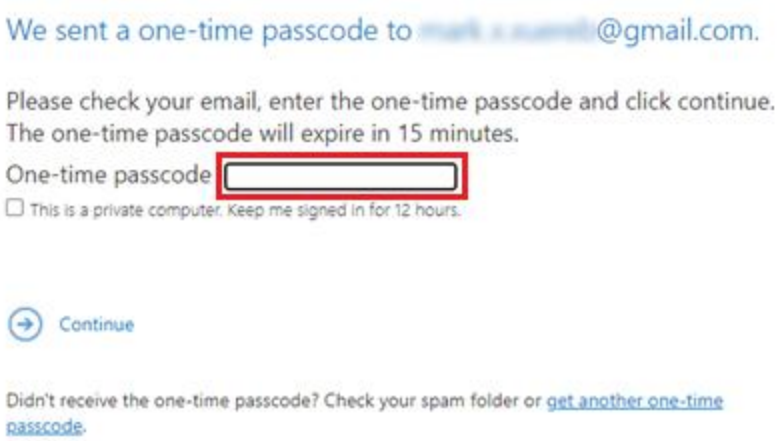
1. When opening the secure email sent from a Government Mailbox, a similar message as shown below, will be displayed



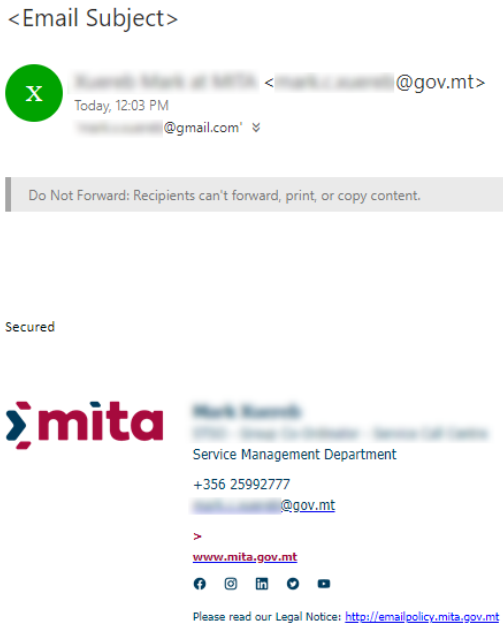
2. Click on the **Read the message** button to open the protected message. This will trigger a new tab to open with the below message



3. Click on **Sign in with a One-time passcode**. An email with a one time passcode will be sent to your Gmail mailbox, Copy the passcode and paste it in the field circuled in red below

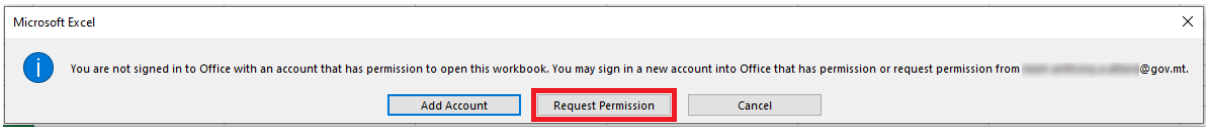


4. Click the **Continue** button to have the protected message displayed



04. Requesting Permissions to view attached files

1. Recipient A, sends and secure email, with an attachment to recipient B as shown in Method 1
2. Recipient B saves the file locally and sends it in a separate email to recipient C (Even if file is renamed)
3. When recipient C received the email (Secured or not) and try to open the original attachment, the below message will prompt

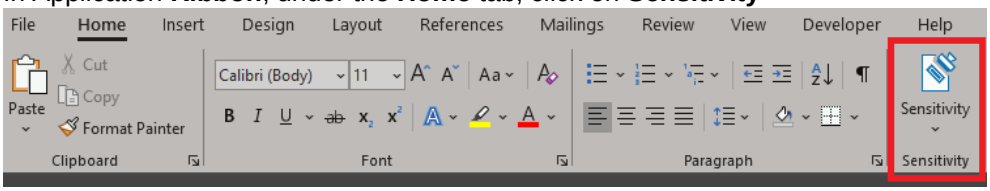


5. Click on **Request Permission**, this will open a new email with the originator email address (recipient A) for recipient C to request permissions
6. The originator can follow instructions in Method 05 to set permissions to recipient C

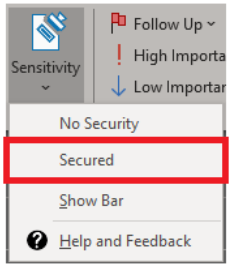
05. Setting permissions on Microsoft Office Applications (Word, Excel, PowerPoint, etc)

1. Open the **Microsoft Application** (i.e. MS Word)

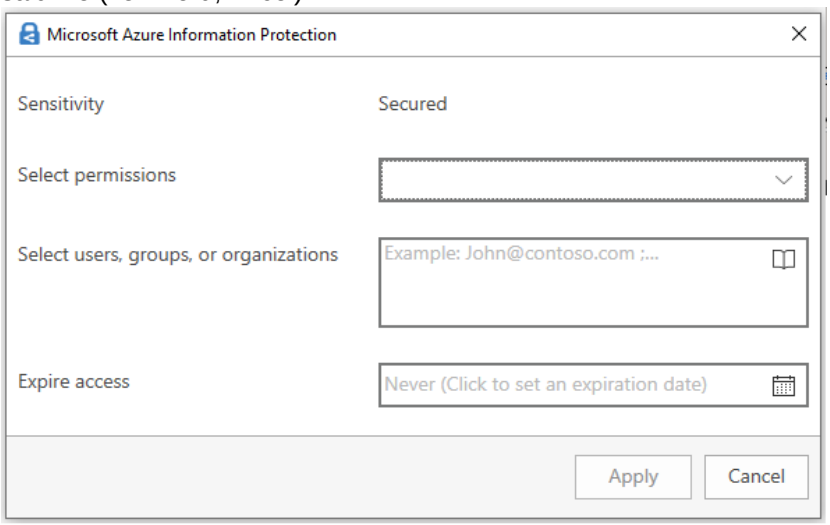
2. In Application **Ribbon**, under the **Home** tab, click on **Sensitivity**



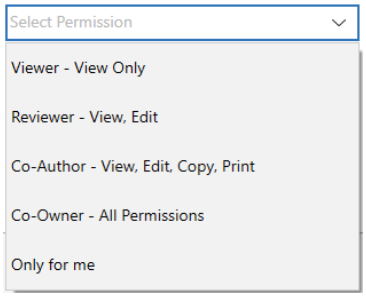
3. Select the **Secured** option



4. The below window will prompt. This is where one can set permission (grant/ revoke) to the said file (i.e. Word, Excel)



   a. **Select Permission**: Using the Drop-Down menu (as shown below), select one of the permissions to set to the file

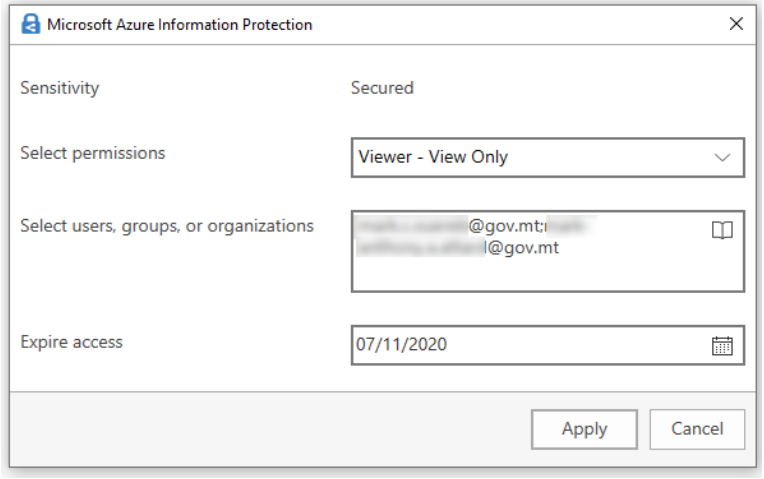


b. **Select users, groups or organisation**: This is where one select the audience of who will have permissions granted/ revoked (Using Email Address).

NOTE: Setting Permissions to **Only for Me**, will not allow you to include any audience.

c. **Expire access**: Select a date when permissions get expired, if left empty, permissions will never be expired.

5. **Once Permissions are set,** you should have details similar to the below



6. Click the **Apply** button to save permissions and close the window

06. Modification History

Version	Date	Author	Comments
Draft 0.1	04/11/2020	Mark Xuereb	Draft version for internal review
Version 1.0	dd/mm/yyyy		First version for release

07. Authorisation

Issuing Authority	Approval Authority
Signature and Date: **Name: Mark Xuereb** **Position: Team Leader**	**Signature and Date:** **Name: Keith Mallia** **Position: Service Manager**