Lab 7 - Microsoft Information Protection

Lab Overview: Microsoft Information Protection

The growth and mobility of data, across devices, apps, cloud services and on-premises, has made protecting sensitive information more challenging than ever. Internal security requirements and evolving compliance regulations have heightened the importance on implementing a comprehensive information protection strategy. Microsoft Information Protection enables you to protect your sensitive information, wherever it lives or travels, across devices, apps, cloud services and on-premises.

Our solution leverages the power of its unified platform to protect and manage sensitive data across its lifecycle: **Discover** and understand where sensitive information resides; **classify & label** files and emails based on sensitivity; apply **protection** based on flexible policies; and **monitor** your sensitive data landscape for potentially risky or undesirable activity. Microsoft Information Protection solutions are easy for IT admins to configure and manage, and they provide comprehensive analytics to better understand your sensitive data landscape and take corrective action. Protection capabilities are built natively into productivity apps and services, giving end-users a consistent and simple approach to securing their information, without inhibiting their productivity.

Microsoft Information Protection refers to a set of products and integrated capabilities. Individual products and capabilities that are typically included as part of the Microsoft Information Protection discussion are Azure Information Protection, Office 365 Information Protection (e.g. Office 365 DLP), Windows Information Protection and specific capabilities in Microsoft Cloud App Security.

Intended Audience

Security IT admins, CISOs

Lab Overview

This lab focuses on showing you the features of MIP and DLP. These are shown below:

- Pre-Requisites
- Part 1 – Configure Sensitivity Labels and DLP Policy
- Part 2 – Test End User
- Part 3 – Send a Protected Email
- Part 4 – Prevent sharing DLP

Lab Pre-requisites

Step1 – Create Demo Tenant

Before you start you should have completed the "Getting started with Labs". If you have not completed this, you will not be able to do this lab. You can find this document which you can download from https://aka.ms/secpractice-labs.

Each tenant can take up to 24 hours to provision so it's important that you complete this prior to when the labs are to be run.

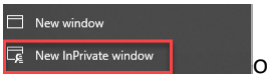
NB – If you already created your demo tenant as part of the Identity Labs you DO NOT need to do this again.

Step 2 – Create yourself an Admin account for your demo tenant.

*NB – If you already created your **ADMIN ACCOUNT** as part of the Identity Labs you DO NOT need to do this again. Please use the same account that you created in the Identity labs. Go straight to Part 1*

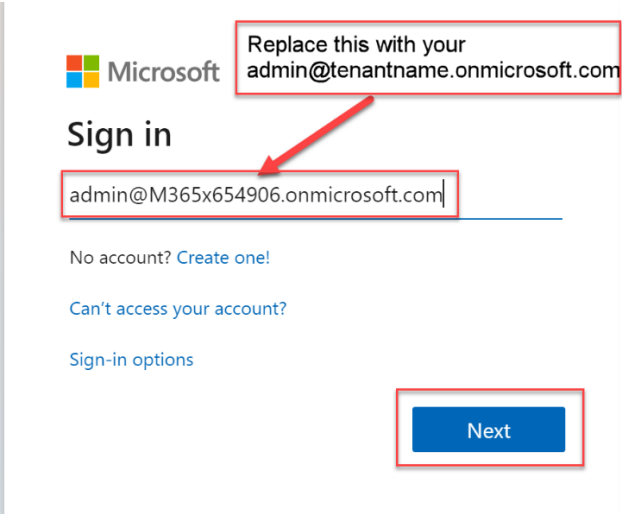
In this task, you will create a Microsoft 365 user account for yourself, and assign your account the Microsoft 365 Global Administrator role, which gives you the ability to perform all administrative functions within Microsoft 365.

Important: As a best practice in your real-world deployments, you should always write down the first global admin account's credentials (in this lab, the MOD Administrator) and store it away for security reasons. This account is a non-personalized identity that owns the highest privileges possible in a tenant. It is **not** MFA activated (because it is not personalized) and the password for this account is typically shared among several users. Therefore, this first global admin is a perfect target for attacks, so it is recommended to create personalized service admins and keep as few global admins as possible. For those global admins that you do create, they should each be mapped to a single identity, and they should each have MFA enforced.

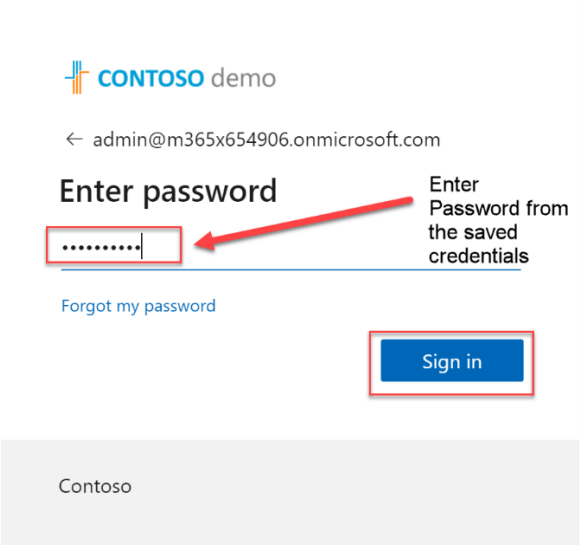
1. Open an In-private browser (Edge) 

or New in-Cognito (Chrome) 

on your machine and then go to https://admin.microsoft.com/
2. Enter the admin account username that you saved in "Getting started with Microsoft Labs" to gain credentials.
3. Enter your admin credentials in the sign in as below and click NEXT



4. Enter the password and then click "Sign in"



5. In the **Microsoft 365 admin center**, in the left navigation pane, select **Users** and then select **Active users**.
6. In the **Active users** list, you will see the default **MOD Administrator** account as well as some other user accounts.
7. In the **Active Users** window, select **Add a user**.
8. In the **Set up the basics** window, enter the following information:

-
  - First name: **Your First Name**
  - Last name: **Your Last Name**
  - Display name: When you tab into this field, **YOUR NAME** will appear.
  - Username: When you tab into this field, **YOURFIRSTNAME-LASTNAME** may appear; if not enter this as the username

IMPORTANT: To the right of the **Username** field is the domain field. select the **M365xZZZZZZ.onmicrosoft.com** cloud domain.

After configuring this field, **YOUR username** should appear as:

YOURNAME@M365xZZZZZZ.onmicrosoft.com

  - Password settings: select the **Let me create the password** option.
  - Password: **Set your own complex Password**
  - Uncheck the **Require this user to change their password when they first sign in** checkbox.
9. Select **Next**.
10. In the **Assign product licenses** window, enter the following information:
11. Select location: **United States (Your Location)**
12. Licenses: Under **Assign user a product license**, select **Office 365 E5** and **Enterprise Mobility + Security E5** or if you have **Microsoft 365 E5** select this instead.
13. Select **Next**.
14. In the **Optional settings** window, in the Roles section select **Admin center access** By doing so, all the Microsoft 365 administrator roles are now enabled and available to be assigned.

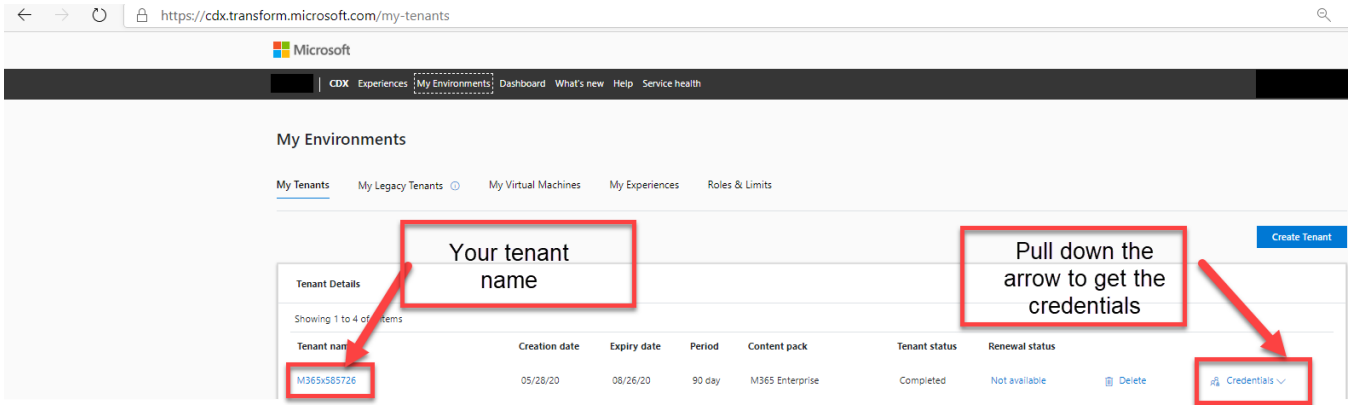
15. Select **Global Admin** and then select **Next**.
16. On the **Review and finish** window, review your selections. If anything needs to be changed, select the appropriate **Edit** link and make the necessary changes. Otherwise, if everything is correct, select **Finish adding**.
17. Once your new username **has been added to active users** page, select **Close.**

Step 3 - Lab Personas

The recommended lab personas to use for in this guide, unless otherwise stated, are:

- Administrator scenarios: **admin@<tenant>.onmicrosoft.com**
- End user scenarios: Isaiah Langer, **IsaiahL@<tenant>.onmicrosoft.com and Allan DeYoung@<tenant>.onmicrosoft.com**

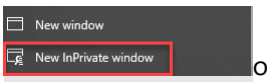
The default password for all users can be found on your tenant information card at https://cdx.transform.microsoft.com

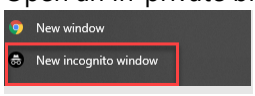


- Create a Gmail account (or other 3rd party email system not managed by Microsoft) to be used for the **Send Protected Message to a Gmail User** and **Block sharing**

Part 1 - Configure Sensitivity Labels and DLP Policy

Objective - Use Microsoft Information Protection or Office 365 to set up your sensitivity labels and protection policies to protect sensitive documents and email. Configure data loss prevention policies to block the accidental or inappropriate sharing of sensitive information.

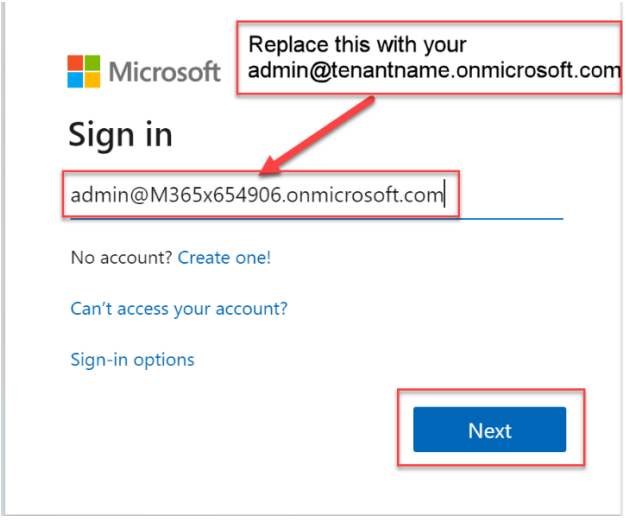
a) Open an In-private browser (Edge) 

or New in-Cognito (Chrome)


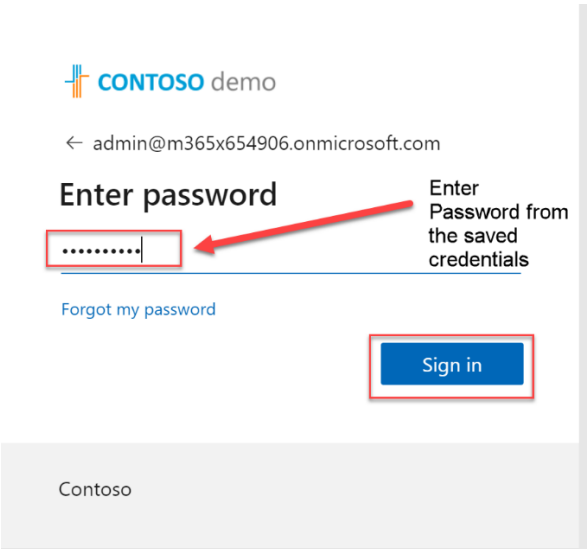
on your machine and then go to https://compliance.microsoft.com/

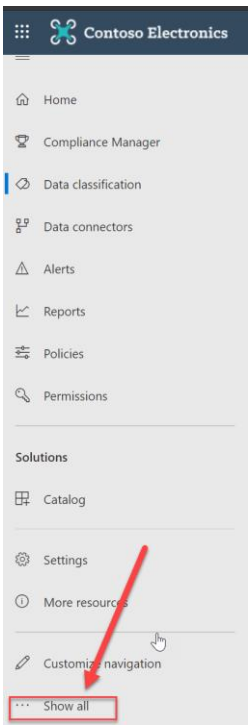
b) Enter the admin account username that you saved in "Getting started with Microsoft Labs" to gain credentials.

c) Enter your admin credentials in the sign in as below and click NEXT



d) Enter the password and then click "Sign in"



Notes	Steps
Unified sensitivity label management in Security & Compliance Center In this scenario, the admin will create a new sensitivity label that will be used to protect confidential information. You can create an encryption policy immediately while creating the label or add it later. The admin will select to encrypt email messages and files, as well as give permissions to users and groups. Only the users and groups selected will be assigned permissions to use the content that has this label applied. The admin will search for a group and select Project Falcon. After encryption has been configured, the content will be marked and managed. Enabling content marking you can add custom headers, footers, and watermarks to the content that has this label applied. After content marking has been configured, you'll manage data loss prevention on the endpoint, specifically Windows 10 machines.	1. In the Security & Compliance portal https://compliance.microsoft.com/ (as above), in the left-hand navigation, navigate to the bottom click on the… and choose **Show All**  2. 3. click **Information Protection Tab**. 4. Click **Labels**. 5. At the top, click **Create a New label**. 6. On the **Name your label** page, create a label as follows: • Label name: **Lab 7 Confidential-PCI** • Description for users: **This content contains sensitive personal information** 7. Click **Next**. 8. On the Encryption page, under **Encryption** click **Apply**, to enable. 9. Under Assign permissions now or let users decide **– Select Assign Permissions now.** 10. Leave **User access to content expires** as default (Never)

Notes	Steps
During the final review of the settings, you can edit specific settings or choose to create the label. After the label is created, settings can still be edited, the label can be published or deleted. Now that the label has been creating and configured, it can be applied automatically or by the user, and the content will be protected based on the settings configured.	11. Leave **Allow offline access** as **Always** 12. Under Assign permissions to specific users and groups – click assign permissions. 13. Click **+ Add users or groups**. 14. In the Search text box, type **Project**, click **Project Falcon**, and then click **Add**. 15. In the Search text box, type **Project**, click **MOD Administrator Account**, and then click **Add**. 16. click **Save**. 17. Click **Next** 18. On the **Content marking** page, click **the switch** to enable. 19. Next to **Add a watermark**, click the check box, and then click **Customize text**. 20. In the **Watermark text** field, type **C O N F I D E N T I A L**, and then click **Save**. 21. On the **Content marking** page, click **Next**. 22. On the **Auto labeling** page, click **the switch** to enable. 23. Under **Detect content that matches these conditions**, click **+ Add a condition**, and then click **Content contains**. 24. Under **Content contains**, click the **Add** drop-down list, and then click **Sensitive info types**. 25. Select Sensitive info types as follows: • **Credit Card Number** • **U.S. / U.K. Passport Number** • **U.S. Bank Account Number** • **U.S. Driver's License Number** • **U.S. Individual Taxpayer Identification Number (ITIN)** • **U.S. Social Security Number** 26. Click **Add**. 27. On **When content matches these conditions** Select **Automatically apply this label** 28. On **Display this message to users when the label is applied – Display this message to**

Notes	Steps
	users when the label is applied enter the following text "**Sensitive information discovered - please review data and confirm you comply with company policy"** 29. Click **Next**. 30. On the **Review your settings** page, verify the options selected, and click **Create Label**
Publish the Label In order to apply the label to users we need to publish this.	1. Return to the **Information Protection Tab**. 2. Click **Label Policies Tab** 3. Click **Publish Label** **4.** On the **Choose sensitivity labels to publish** wizard Select "**Choose sensitivity labels to publish"** 5. Wait for the Search to populate then Select the label you created "**Lab 7 Confidential -PCI"** 6. Select **Add and then Next** 7. In the **"Publish to users and groups"** Select choose **users and groups** 8. Select **the +Add button** 9. Add your **Admin account**, **MOD Administrator** and **Project Falcon Group** 10. Select **Done** 11. Click **Next** 12. Under **Policy settings,** pull down the drop box and Add the Label we created **Lab 7 Confidential -PCI.** 13. Select the tick box for "**Users must provide justification to remove a label or lower classification Label**." 14. Click **Next** 15. Name the Policy "**Lab 7 – Policy**" 16. Click **Next** 17. Then Click **Submit**
Configure Office 365 Data Loss Prevention in Security & Compliance Center	

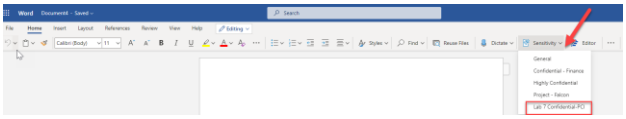
Notes	Steps
To comply with business standards and industry regulations, organizations need to protect sensitive information and prevent accidental oversharing and leakage. With an **Office 365 data loss prevention (DLP) policies**, you can prevent the inappropriate sharing of sensitive information. The admin will use the **General Data Protection Regulation (GDPR)** template, to create a DLP policy to identify personal information inside the European Union (EU). Using a DLP policy, you can: • Detect sensitive information across many locations, including email in Exchange Online, and documents in SharePoint Online and OneDrive for Business, and in the desktop versions of Excel, PowerPoint, Word and Outlook. • Prevent the accidental sharing of sensitive information. • Monitor policy violations for further investigation. • Help users learn how to stay compliant without interrupting their workflow with notifications and "policy tips". A DLP policy contains a few basic settings: • Where to protect the content - locations such as Exchange Online, SharePoint sites, and OneDrive accounts, and Microsoft Teams chats. • Conditions for applying policy, such as a match against one of the over 80+ sensitivity information types, or your own custom sensitive information types. • When and how to protect the content by enforcing rules. After you have created the policy, you have the option of turning on the policy or testing it first.	1. In the Compliance portal, in the left-hand navigation, click **Data loss prevention**. 2. Click **Policy**. 3. Click **+ Create a policy**. 4. On the **Start with a template or create a custom policy** page, click **Privacy**, click **General Data Protection Regulation (GDPR)**, and then click **Next**. 5. On the **Name your Policy** page, Enter **Lab 7-General Data Protection Regulation (GDPR)** and click **Next**. 6. On the **Choose locations** page, review the locations, and Turn Off Devices 7. Click **Next**. 8. On the **Define policy settings** page, click **Create or customize advanced dlp rules**, and then click **Next**. 9. On the **Customize the type of content you want to protect** page click **Low volume content detected** rule. 10. Click **Edit rule**. 11. On the **Low volume EU Sensitive content found Change** the settings as follows: • Conditions > Content is shared from Microsoft 365: change to **with people inside my organization** 12. **Actions** > Restrict access or encrypt the content: **Block people from sharing and restrict access to shared content** 13. Click **Save**. 14. On the **Customize the type of content you want to protect** page, click **Next**. 15. On the **Do you want to turn on the policy or test things out first** click **Yes, turn it on right away** and click **Next**. 16. On the **Review your settings** page, verify the options selected, and click **Submit**. 17. On the **General Data Protection Regulation** page, click **Submit**.

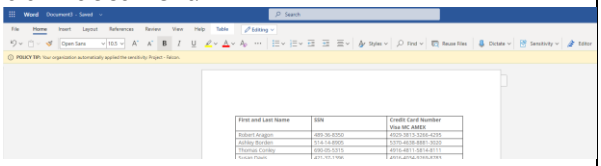
Notes	Steps

End of Part 1

Part 2 – Test End User Native Sensitivity Labeling in Office Online

Microsoft is improving the information protection experience for its end-users by making it easy to add sensitivity labels to their documents and emails. The easier it is to do, the more likely they are to classify information correctly.

Notes	Steps
### Labeling in Office In Office apps sensitivity labels appear on the Sensitivity button, on the Home tab, and on the Ribbon. The label applied also appears in the Status bar at the bottom of the window. After a sensitivity label is applied to an email or document, the protection settings for that label are enforced on the content. Lets imagine, You've added details about a fundraiser that you're planning, and you know your company has policies to classify and apply the correct sensitivity label to any document, even if it doesn't contain sensitive data. Right within Word online, you can use the new, built-in label picker to easily select the right label that's appropriate for this document. Using the Sensitivity drop-down menu, you can apply the "Highly Confidential" label. The sensitivity label is applied to the document, and the Highly Confidential watermark is also added to the document. Next, we'll review how this works in Excel. Similar to Word, in Excel, you can use the new, natively integrated label picker to easily select the right label that's right for this document. Using the drop-down menu, you can apply "Confidential-Finance" label. The sensitivity label is added to the document's properties. The new, natively integrated label picker to easily select the right label is now available in Outlook for email also. Using the drop-down menu, you can apply the "Highly Confidential" label. When this email is sent, the receiver will see that the email is protected. The header of the email contains information indicating that it is Confidential. The header information displayed can be customized by IT admins.	1. In the same Inprivate or Icognito browser go to https://www.office.com/ 2. Log in as your Admin User (MOD Administrator" 3. On the left hand side of the screen. Click the **Word** icon (left Tab) 4. Click **+** button to create a New Blank Document 5. On the **HOME** screen tab, In the top-right corner, click **Sensitivity**. You will see some pre-built labels in the demo platform. *Note: The label you created above will appear here too after about 5 minutes. You may need to create a new Blank document to see it populate*  6. Go to this URL in another browser. https://dlptest.com/sample-data/

Notes	Steps
	7. Paste the fake data from the URL below into the blank document:  8. You should see the Policy Tip appear as above 9. The "Project Falcon" Policy applies first as it has higher preference than the one we just created.

END OF PART 2

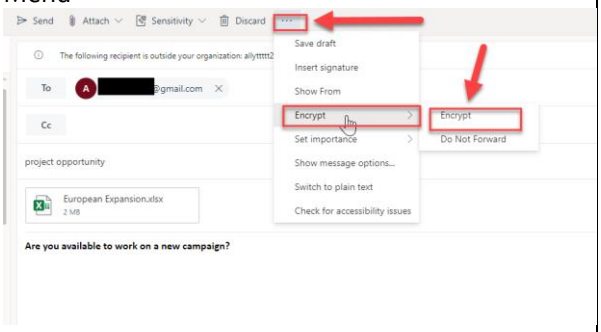
Part 3 - Send a Protected Email to an External User

People often use email to exchange sensitive information, such as financial data, legal contracts, confidential product information, sales reports and projections, patient health information, or customer and employee information. As a result, mailboxes can become repositories for large amounts of potentially sensitive information, and information leakage can become a serious threat to your organization.

Office 365 Message Encryption enables users to send protected email messages to people inside and outside the organization. Protected emails easily work with users across a variety of services, including Office 365, Outlook.com, Gmail, Yahoo, and other email services.

Recipients can read and respond to messages protected by Office 365 Message Encryption no matter what email provider they use.

Notes	Steps
Send Protected Email to a Gmail User Isaiah needs to communicate with a PR firm about an upcoming ad campaign at Contoso. The PR firm uses Gmail as their email provider. You can create policies that enforce encryption on all email messages sent to external recipients, so when a new message is composed to an external recipient, it is automatically protected.	1. Launch an InPrivate session in the web browser and navigate to **https://portal.office.com**. 2. Sign in as **IsaiahL@<tenant>.onmicrosoft.com** using the tenant password from demo card on cdx.transform.microsoft.com. 3. On the Office 365 portal, click **Outlook**. 4. Click **+New message**. 5. In the **To** line, type the external Gmail address created during setup.

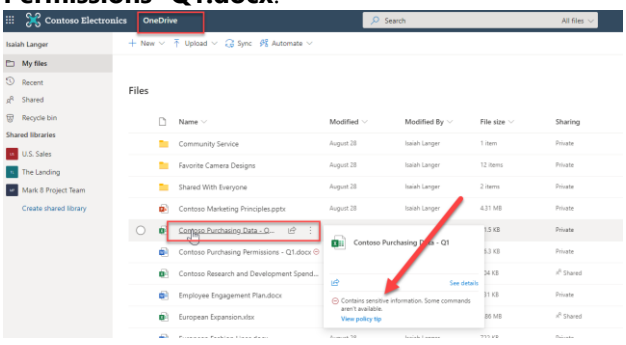
Notes	Steps
For this scenario, Isaiah will manually encrypt the email being sent to an external recipient. Gmail is not RMS-aware, so when Alex receives the message, it's wrapped in another email that provides instructions on how to read it. Because Alex is using Gmail, he has the option of using the new federated sign-in experience to read this message. When he signs in with his Gmail credentials, the message is displayed. And no matter what email provider the recipient uses, they can always read an encrypted message by requesting a one-time key.	6. In the **Subject** line, type **Project opportunity**. 7. Click the **Attachment** icon ( ). 8. Click **Cloud locations**. Then choose **Files** 9. Select **European Expansion.xlsx** and click **Next**. 10. Click **Attach as a copy**. 11. In the message body, type **Are you available to work on a new campaign?** 12. From the Menu Pane Select the … and pull down Menu  13. Click **Encrypt**. 14. Click **Send**. 15. On a new browser Session, navigate to **http://gmail.com**. Sign in as the Gmail user created in the pre-reqs steps. 16. Click on the new message from Isaiah Langer. 17. Click **Read the message**. (*If you get an error reading the message you may be logged in with multiple identities. Please ensure you created a new Browser session when logging onto google account)* 18. If required, click **Sign in with Google** and follow the sign in steps. 19. In the email, click **European Expansion.xlsx**.

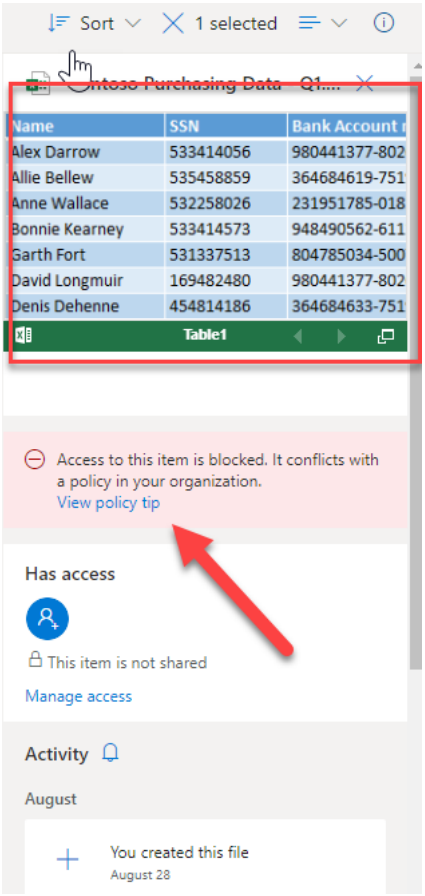
Part 4 - Prevent Sharing of Sensitive Data with Office 365 Data Loss Prevention

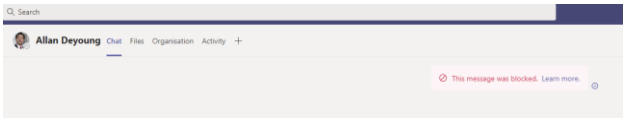
To comply with business standards and industry regulations, organizations need to protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII), such as credit card numbers, social security numbers, or health records. With a **Data Loss Prevention (DLP)** policy in the Office 365 Security & Compliance Center, you can identify, monitor, and automatically protect sensitive information across Office 365.

With a DLP policy, you can:

- Identify sensitive information across many locations, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.
- Prevent the accidental sharing of sensitive information.
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word.
- Help users learn how to stay compliant without interrupting their workflow.
- View DLP reports showing content that matches your organization's DLP policies.

Notes	Steps
Block sharing of sensitive information from SharePoint Online Data loss prevention in Office 365 helps organizations protect their sensitive data across their Office 365 environment, including Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams. Contoso has strict requirements to protect various types of data for regulatory, policy, or privacy reasons. They use Office 365 Data Loss Prevention policies to help achieve this goal. For example, when Isaiah Langer accesses his OneDrive for Business folders, he sees this icon on a document he owns. This warning tells him that this document has been flagged by a DLP policy. In this case, the document has been flagged because it contains credit card information. Isaiah wants more information, so he looks at the document properties. Here he can get more information. He can also report this to an administrator if he thinks the policy is been applied in error.	1. Launch an **InPrivate** session in the web browser and navigate to **https://portal.office.com**. 2. Sign in as **IsaiahL@<tenant>.onmicrosoft.com** using the tenant password from **cdx.transform.microsoft.com** 3. On the Office 365 portal, click **OneDrive** 4. Hover over the files **Contoso Purchasing Permissions -Q1.docx**.  5. Click **View policy tip** and review the reason the label was applied.

Notes	Steps
When Isaiah tries to share the content, he is informed that the item contains sensitive information and can't be share outside the organization.	6. In this view you can see the policy view as well as a preview of the data that shows the reason the policy has been applied  7. 8. Close the **Tip**
## Block sharing of sensitive information from Teams Data loss prevention (DLP) has been available for Exchange Online, SharePoint Online and OneDrive for Business for a while, and DLP has been recently extended to Microsoft Teams, to enable the blocking of sensitive information contained in chat messages and channel conversations. This is based on the same policy engine used and proven in our other DLP services. When someone sends a message, either within a chat or a channel, the content of the message is inspected for sensitive information in near real-time. If sensitive	**Setup additional test account – do not logout Isaiah** 1. Launch an InPrivate session in the web browser and navigate to https://portal.office.com. 2. Sign in as AllanD@<tenant>.onmicrosoft.com using the tenant password from on cdx.transform.microsoft.com 3. On the Office 365 portal, click Teams. Teams will open in separate tabs. 4. On the Teams tab, click Use the web app instead.

Notes	Steps
information is identified, then the message is revoked and no longer accessible by the recipient(s). Similar to how DLP operates in other Office 365 services, policy tips give the sender additional information on the reason for the message being blocked, such as the presence of passport information or social security numbers. End-users can override the blocked message or report the issue as a false positive, if allowed by IT. For organizations that are using Microsoft Teams to accelerate their workforce collaboration and productivity, this provides a new way to ensure proper control and governance of important data – both for the purpose of achieving internal security objectives as well as meeting external compliance and privacy requirements.	1. In the other Browser you should still be logged in as Asaigh 2. On the Office 365 portal, click **Teams** 3. On the Teams tab, click **Use the web app** instead. 4. On the browser with Teams open, in left hand navigation, click Chat, and then click Allan Deyoung. 5. Switch to the browser with **Teams** open. 6. In the chat with **Allan Deyoung**, type **EU Passport number x13256730**, and then click **Send**.  7. There may be a delay but you should see, **This message was blocked**.  8. Switch to the other InPrivate browser with Teams open as Allan Deyoung 9. Switch to the browser with Teams open. 10. In the chat with you should see the blocked message from Isaiah.

End of LAB