Data Loss Prevention

Summary

Overview: Data Loss Prevention (DLP) in Microsoft Teams, as well as the larger DLP story for Microsoft 365 or Office 365, revolves around business readiness when it comes to protecting sensitive documents and data. Whether you have concerns around sensitive information in messages or documents, DLP policies will be able to help ensure your users don't share this sensitive data with the wrong people. In this lab guide, you will learn how to add Microsoft Teams to an existing DLP policy, as well as create a new policy, whether based on a template or fully customized to your organsiation's data protection needs.

Lab steps

What is it	Where is it and what to do
Configuring DLP policies for Microsoft Teams Data Loss Prevention (DLP) in Microsoft Teams, as well as the larger DLP story for Microsoft 365 or Office 365, revolves around business readiness when it comes to protecting sensitive documents and data. Whether you have concerns around sensitive information in messages or documents, DLP policies will be able to help ensure your users don't share this sensitive data with the wrong people. In this guide, you will learn how to add Microsoft Teams to an existing DLP policy, as well as create a new policy, whether based on a template or fully customized to your organization's data protection needs.	Navigate to https://compliance.microsoft.com logged in as the administrator of your given demo tenant. Login with the credentials you have been provided for your lab tenant
Exercise 1: Create a new DLP Policy from a template In this example, you will create a new DLP policy starting with a template. By starting with a DLP template, you save the work of building a new set of rules from scratch and figuring out which types of information should be included by default. You can then add to or modify these requirements to fine tune the rule to meet your organization's specific requirements.	1. Starting on the Data loss prevention section in the Microsoft 365 compliance admin center, click on Policies, then click on the **+ Create policy** button 2. Under Categories, select **Privacy**. **3.** In the Templates list, select **General Data Protection Regulation (GDPR).** 4. Review the template description and then click the **Next** button.

What is it	Where is it and what to do
	5. In this exercise we will be keeping the default name and description, so click **Next** on the Name your DLP policy page. 6. On the **Choose locations to apply** the policy pane, note the defaults, which include Teams chat and channel messages, and click **Next**. 7. On the **Define policy settings** pane, click **Next**. 8. On the Info to protect pane, review the sensitive info types that will be detected and then click **Next**. 9. On **Protection actions**, under Detect when a specific amount of sensitive info is being shared at one time, **change the value from 10 to 1 and hit Enter**. 10. Click the **Next** button on the Protection actions page. 11. On the **Customize access and override settings page**, under Block users from accessing shared SharePoint, Exchange, OneDrive and Teams content, select **Block Everyone**. 12. In this example, we will not be allowing users to override the policy, so click the checkbox next to **Let people who see the tip override the policy** to de-select it. 13. Click the **Next** button at the bottom of the Customize access and override settings page. 14. On the Test or turn on the policy page, select the radio button next

What is it	Where is it and what to do
	to **Yes, turn it on right away**, then click the **Next** button at the bottom of the page. 15. Review your policy settings and then click the **Submit** button. 16. On the New policy created page, click the **Done** button to finalize your changes.
Exercise 2: Create a new custom DLP Policy In this exercise, you will learn how to create a DLP policy based on a custom sensitive info type to protect against disclosure of sensitive information pertaining to a confidential project. You've already created a custom sensitive info type in the previous lab called Customer ID.	1. Select **Policies** in the left navigation of the Microsoft 365 compliance admin center. 2. In the Policies pane, click on **Data loss prevention**. 3. On the Data loss prevention page, select **+ Create policy**. 4. Select **Custom** from the categories or choose a category. Click **Next** 5. On the Name your DLP policy page, click to place focus in the **Name** field, then type **Customer ID (XX) with your unique number (21-100)** and hit Enter. 6. Click to place focus in the Description field, then type or copy and paste **Customer ID Confidential Information Protection Policy** and hit Enter. 7. Click the **Next** button. 8. Review the locations to which the policy will apply, noting that Exchange is included, then click the **Next** button.

What is it	Where is it and what to do
	9. On the **Define policy settings** page, ensure that the **create or customize advanced DLP rules** is selected then click the **Next** button. 10. On the Customize advanced DLP rules page, click the **+ Create rule** button. 11. On the Create rule panel, click to place focus in the **Name** field and then type **Customer ID sensitive content detection** and hit Enter. 12. Under Conditions, click the **+ Add condition** button and then select **Content contains** from the dropdown list. 13. Under Content contains, select **Add** and then select **Sensitive info types**. 14. On the Sensitive info types panel, click to place focus in the Search field, then type **Customer ID** and hit Enter. 15. Click the checkbox to select the Customer ID XX (the same one you created in the previous lab). Confidential information from the results list, and then click the **Add** button. 16. Click to scroll down, and then under User notifications, **set the toggle to On** to Use notifications to inform your users and help educate them on the proper use of sensitive info. 17. Under Policy tips, select the checkbox to Customize the policy tip text. 18. In the custom policy tip text field, type or copy/paste **This content appears to contain sensitive**

What is it	Where is it and what to do
	information: Customer ID. Business justification is required to override. and hit Enter. 19. Under **User overrides**, click the toggle switch to let people who see the tip override the policy and share the content. 20. Select the check box to Require a business justification to override. 21. Click to scroll down, and then Under incident reports, select the severity dropdown and then select **Medium**. 22. Set the toggle switch to On to Send an alert to admins when a rule match occurs. 23. Click to scroll down and then click the **Save** button. 24. On the Customize advanced DLP rules page, click the **Next** button 25. On the Test or turn on the policy page, select the radio button next to **Yes, turn it on right away**, then click the **Next** button 26. Review your custom policy settings and then click the **Submit** button 27. Click the **Done** button on the New policy created page to finalize your changes.
Exercise 3: End User Experience	1. Starting in Outlook Online (Waffle icon top left -> Outlook), logged in as your user still - a Contoso employee in the HR department, start to create a new email.

What is it	Where is it and what to do
In this exercise, you will see the user experience for the custom DLP policy you created in exercise 3.	2. Click on New Message, in the To field, type in an Outlook mail address, e.g. Megan@outlook.com 3. In the subject type: Content attached, and in the body of the email copy and paste) Or type: Content attached. 4. Next, Click on Browse Cloud Locations, click on Groups, then locate Sales & Marketing. 5. Locate the "Sensitive data" folder, and choose the file names **Customer ID.docx**. 6. The file attaches to the email, and you can now hit send. 7. Notice the policy tips that appear stating that the email recipient is outside of your organization, and a following new email that comes into the mailbox stating the email was not sent. 8. This has now protected potentially sensitive information from being accidentally or maliciously sent from your organization.
Exercise : Reporting You will then learn how to use the Microsoft 365 compliance admin center to access reports on DLP policy matches and incidents. Now, we willl switch to the administrator perspective to access the reports corresponding to Megan's message, as well as other DLP policy matches in the organization.	1. Navigate to 2. compliance.microsoft.com 3. Login with the credentials you have been provided for your lab tenant 4. Select **Reports** in the left navigation. 5. On the Reports page, **click to scroll down** to the DLP related reports, where you have at-a-glance visibility into DLP related metrics across Teams, Exchange, SharePoint and OneDrive for Business.

What is it	Where is it and what to do
	6. Click on **View details** in the DLP Policy Matches tile. 7. In the list of policy matches, note that both the chat message sent by Megan and the document she had uploaded to OneDrive and shared are present in the report. **Click on the message sent by Megan** to view more detail. 8. Review the additional detail and then click the **Close** button. 9. Click on Reports in the upper left of the Reports > DLP Matches page to return to the dashboard. 10. Click on **View details** in the DLP Incidents tile. 11. The DLP incidents report provides a view across workloads, providing insight into severity and details regarding the incident(s). Click on the **Customer ID X** to view more detail regarding that incident. 12. The DLP incidents report provides a view across workloads, providing insight into severity and details regarding the incident(s). Click on the **Customer ID reference doc** to view more detail regarding that incident.
Summary - Congratulations on completing the Interactive Guide! You're now ready to configure and validate DLP policies for Microsoft Teams and other Microsoft 365 workloads.	