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 interactive 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 organziation's data protection needs.

Exercise 1: Add Microsoft Teams as a location to an existing policy

In this exercise, you will use the Microsoft 365 Compliance admin center to edit an existing DLP policy, adding Microsoft Teams as a location to which the policy will apply.

The exercise begins in the M365 admin center (https://admin.microsoft.com) logged in as the administrator of Contoso.

1. □ Click **Show all** in the left navigation.
2. □ Under Admin centers in the left navigation, select **Compliance** to open the Microsoft 365 Compliance admin center in a new tab.
3. □ In the Microsoft 365 compliance admin center, select **Policies** in the left navigation.
4. □ In the Policies pane, click on **Data loss prevention**.
5. □ Hover over US Personally Identifiable Information (PII) Data and click on the circle in the left hand column to select that policy.
6. □ Click the **Edit Policy** button.
7. □ Click **Next** on Name your DLP policy pane.
8. □ On the Choose locations to apply the policy page, set the toggle switch for Teams chats and channel messages to On.
9. □ To start, you will only be rolling out this change to the IT department at Contoso to validate the behavior within Microsoft Teams before deploying more broadly. In the Included column, next to Teams chat and channel messages, select **Choose account**.
10. □ On the Teams chat and channel messages panel, click to place focus in the Search field, then type **IT** and hit Enter.
11. □ Click the checkbox to select **Contoso IT department** from the results list, then click the **Done** button.
12. □ On the Choose locations to apply the policy page, note that 1 account will be included. The option to include or exclude individuals and groups with DLP policy provides the flexibility you need to meet your organizations requirements, whether it is limiting initial scope to a test group (as in this exercise) or applying a policy only to specific groups who must meet certain regulatory requirements. When you are ready, click the **Next** button.

13. □ On the Customize advanced DLP rules page, click the **Next** button
14. □ On the Test or turn on the policy page, click the **Next** button
15. □ Review your policy settings and then click the **Submit** button
16. □ Click the **Done** button to finalize your changes.

Exercise 2: 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 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.
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, 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 to **Yes, turn it on right away** and 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 3: 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.

Part 1: Create a custom sensitive info type for the Mark 8 project

1. □ Starting on the home page of the Microsoft 365 compliance admin center, select **Data classification** in the left navigation.
2. □ On the Data classification page, click on the **Sensitive info types** tab.
3. □ Click the **+ Create info type** button.
4. □ On the Choose a name and description page, click to place focus in the Name field and then type **Mark 8 Confidential Information** and hit Enter.
5. □ Click to place focus in the Description field and paste in **Content containing sensitive information pertaining to the confidential Mark 8 project** and hit Enter.
6. □ Click the **Next** button.
7. □ On the Requirements for matching page, click the **+ Add an element** button.
8. □ Under Matching element, click to expand the **Detect content containing** menu and then **select Keywords**.
9. □ Click to place focus in the Enter keyword list field and then type **Mark 8, architecture, implementation, contract** and hit Enter.
10. □ Click to scroll down and then hit the **Next** button
11. □ Review your sensitive info type settings and then click the **Finish** button.
12. □ Click **No** on the compliance dialog, as we will not be testing the new sensitive info type in this exercise. You have now created a custom sensitive info type and are ready to use it to create a new custom DLP policy.

Part 2: Create a custom policy

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. □ Click **Next** on the Start with a template or create a custom policy.
5. □ On the Name your DLP policy page, click to place focus in the **Name** field, then type **Mark 8 Confidential Information Protection Policy** and hit Enter.
6. □ Click to place focus in the Description field, then type or copy and paste **Data Loss Prevention policy implemented to prevent unauthorized sharing of confidential Mark 8 project information.** and hit Enter.
7. □ Click the **Next** button.

8. □ Review the locations to which the policy will apply, noting that Teams chat and channel messages is included, then click the **Next** button.
9. □ On the Define policy settings page, 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 **Mark 8 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 **Mark 8** and hit Enter.
15. □ Click the checkbox to select Mark 8 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 then on the proper user 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 information regarding the Mark 8 project. 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 4: End User Experience and Reporting

In this exercise, you will see the Microsoft Teams user experience for the custom DLP policy you created in exercise 3. You will then learn how to use the Microsoft 365 compliance admin center to access reports on DLP policy matches and incidents.

Part 1: Teams user experience

1. □ Starting in Microsoft Teams, logged in as Megan Bowen - a Contoso employee in the marketing department, select **Chat** in the left navigation.
2. □ In Chat, continue the conversation with Alex by clicking to place focus in the new message field, then typing **Here's the copy of the Mark 8 architecture / design doc you wanted.** and hitting Enter.
3. □ Add a file by clicking on the **attachment (paperclip)**
4. □ Select OneDrive, and then select the **Mark 8 architecture reference doc** from the list.
5. □ Click the Share button.
6. □ Click the Send button in the lower right.
7. □ Shortly after sending the message, you will see that the message has been flagged.

Part 2: Admin reporting experience

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. □ Select the Microsoft Edge icon in the Windows Taskbar to switch to the Microsoft 365 compliance admin center in Edge.
2. □ Select **Reports** in the left navigation.
3. □ 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.
4. □ Click on **View details** in the DLP Policy Matches tile.
5. □ 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.
6. □ Review the additional detail and then click the **Close** button.
7. □ Click on Reports in the upper left of the Reports > DLP Matches page to return to the dashboard.
8. □ Click on **View details** in the DLP Incidents tile.
9. □ The DLP incidents report provides a view across workloads, providing insight into severity and details regarding the incident(s). Click on the **Mark 8 architecture reference doc** to view more detail regarding that incident.
10. □ In the details, you can see that this is the document Megan uploaded to OneDrive for Business and that it contains 3 counts of sensitive information. Click the **Close** button when you are done reviewing the details.

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.

To continue your learning with Microsoft Teams we highly recommend navigating to aka.ms/TeamsonLearn.