Managing Compliance in Teams

Introduction

In this Interactive Guide, you will use the Microsoft 365 Security, Microsoft 365 Compliance, and Microsoft Teams admin centers, as well as Windows PowerShell to manage and configure an Office 365 organization's Microsoft Teams policies and settings. You will perform administrative tasks focused on compliance.

What you will learn

After completing this lab, you will be able to:

- Create and apply sensitivity labels to Teams
- Create and monitor a new sensitive info type with Communication Compliance
- Create a new data loss prevention (DLP) policy
- Create an information barrier policy

Exercise 1: Create and apply sensitivity labels to Teams

Sensitivity labels allow Teams admins to regulate access to sensitive organizational content created during collaboration within teams. You can define sensitivity labels and their associated policies in the Security & Compliance Center. These labels and policies are automatically applied to teams in your organization. For this exercise, you will be creating a Mark 9 label for highly confidential communications and content and applying that label to the Mark 9 Project team when you create it

Enable Sensitivity Label support in PowerShell

To apply published sensitivity labels to groups, you must first enable the feature and synchronize sensitivity labels with Azure AD.

NOTE: In this interactive guide, the AzureADPreview PowerShell module has already been installed, for me information on how to install the module, consult this document.

1. ☐ Type the following and hit Enter:
   ```
   Import-Module AzureADPreview
   ```
2. ☐ Type the following and hit Enter:
   ```
   Connect-AzureAD
   ```
3. ☐ Authenticate with your administrator credentials.
   - Type admin@contoso.com and hit enter or click Next
   - Type Password and hit enter or click Sign in
4. ☐ Get the current group settings for the Azure AD organization by typing the following and hitting Enter:
   ```
   $Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting | 
   where -Property DisplayName -Value "Group.Unified" -EQ).id
   ```

5. ☐ Type the following and hit Enter to review the current Group settings values:
   `$Setting.Values`
6. ☐ Enable sensitivity labels by typing the following and hitting Enter:
   `$Setting["EnableMIPLabels"] = "True"`
7. ☐ Save your change by typing the following and hitting Enter:
   `Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting`

Synchronize sensitivity labels to Azure AD

1. ☐ First, connect to the Office 365 Security and Compliance Center in Powershell using the EXO V2 module. Load the EXO V2 module by running the following command:
   `Import-Module ExchangeOnlineManagement`

   Note: Learn more about installing and maintaining EXO V2 module in this document.

2. ☐ Run the following command to connect to the Security & Compliance Center:
   `Connect-IPPSSession -Credential $UserCredential -ConnectionUri https://ps.compliance.protection.outlook.com/powershell-liveid/`

   NOTE: The URI you will use depends on the environment, the one we are connecting to in this guide is for Microsoft 365 and Microsoft 365 GCC tenants. Refer to this document for information on URIs for other environments.

3. ☐ Authenticate with your administrator credentials
   - Type **admin@contoso.com** and hit Enter or click Next.
   - Type **password** and hit enter or click **Sign in.**
4. ☐ Run the following command to synchronize your labels to Azure AD to ensure they can be used with Groups:
   `Execute-AzureAdLabelSync`

Create a new sensitivity label for Mark 9 communication and content

1. ☐ Click the Edge icon in the Windows taskbar to switch to the Microsoft 365 admin center in Microsoft Edge.
2. ☐ Click **...Show all** in the left navigation of the Microsoft 365 admin center.
3. ☐ Select **Compliance** in the left navigation to open the Microsoft 365 Compliance admin center in a new tab.
4. ☐ Click **...Show all** in the left navigation of the Microsoft 365 Compliance admin center.
5. ☐ Scroll down in the left navigation and click on **Information Protection**.
6. ☐ On the Information Protection page, click the **+Create a label**
7. ☐ In the New sensitivity label wizard, click to place focus in the Name field, then type **Mark 9 Confidential** and hit Tab or Enter.
8. ☐ In the Description field, type **Label applied to highly sensitive content and discussion regarding the Mark 9 project** and hit Enter.

9. ☐ Click the **Next** button.
10. ☐ On the Encryption page, click to expand the dropdown menu and select **Apply**.
11. ☐ Scroll down and under Assign permissions to specific users and groups, select **Assign permissions.**
12. ☐ On the Assign permissions panel, select **Add all users and groups in your organization**.
13. ☐ Click the **Save** button.
14. ☐ Click the **Next** button in the New sensitivity label wizard.
15. ☐ On the Content marking page, set the **Content marking toggle** to On.
16. ☐ Select the checkbox to **Add a watermark** and then select **Customize text**.
17. ☐ Click to place focus in the Watermark text field, then type **Highly Confidential** and hit Enter.
18. ☐ Click the **Save** button on the Customize watermark text panel.
19. ☐ Click the **Next** button in the New sensitivity label wizard.
20. ☐ Click the **Site and group settings** toggle switch.
21. ☐ Click to expand the menu for **Privacy of Microsoft 365 group connected team sites** and then select **Private – only members can access the site.** This setting with ensure that any groups to which this label is applied will be private.
22. ☐ Under Unmanaged devices, select the radio button to **Allow limited, web only access** and then click the **Next** button.
23. ☐ On the Auto-labeling for Office apps page, click the **Next** button.
24. ☐ Review your settings and then select **Create label** and then select **Done** on the Your label was created page.

Publish your sensitivity label

1. ☐ In the list of labels, select **Mark 9 confidential**.
2. ☐ On the Mark 9 confidential panel, click the **Publish label** button.
3. ☐ In production, it is recommended to limit the number of label policies, which can be achieved by grouping multiple labels together in one policy. For the purpose of this interactive guide we will only be publishing the Mark 9 confidential label, so click the **Next** button.
4. ☐ On the Publish to users and groups page, select **Choose users or groups**.
5. ☐ On the Edit locations panel, click the **+Add** button.
6. ☐ Click to place focus in the Search field, then type **mark** and hit Enter.
7. ☐ Click the checkbox to select the **Mark 9 Engineering** team and then click the **Add** button.
8. ☐ Click the **Done** button.
9. ☐ On the Publish to users and groups page, click the **Next** button.
10. ☐ On the Policy settings page, click to expand the **Apply this label by default to documents and email** menu, then select **Mark 9 confidential**.

11. ☐ Select **Users must provide justification to remove a label or lower classification label** then click the **Next** button.
12. ☐ On the Name your policy page, click to place focus in the Name field and then type **Mark 9 Sensitivity Label Policy** and hit Enter.
13. ☐ Click the **Next** button on the Name your policy page.
14. ☐ Review your settings and click **Submit**, then click **Done** on the New policy created page.

Note: Microsoft recommends waiting one hour for changes to replicate after creating a new label and then applying that label to a test group prior to publishing broadly. To learn more about pre-requisites and best practices when using sensitivity labels to protect content in Microsoft Teams, click here.

Apply a sensitivity label during Team creation and verify the experience

1. ☐ Switch to the **Microsoft Teams** tab in Edge.
2. ☐ Click on **Join or create a team**
3. ☐ On the Join or create a team page, click the **Create team** button.
4. ☐ Select **Build a team from scratch**.
5. ☐ Click to expand the **Sensitivity** menu, then select the **Mark 9 confidential** label.

   Note that after applying the Mark 9 confidential sensitivity label to the team, Private is the only available option in accordance with the label configuration.

6. ☐ In the Team name field, type **Mark 9 Project Team** and hit Enter.
7. ☐ In the Description field, type **Design, implementation and launch of confidential Mark 9 project** and hit Enter.
8. ☐ Click the **Create** button.
9. ☐ On the Add members to Mark 9 project team page, click the **Skip** button.
10. ☐ On the General channel page for the new Mark 9 Project Team, review the sensitivity labelling in the upper right and click on **Mark 9 confident…** – indicating this team is private and labelled Mark 9 confidential.
11. ☐ Select the **Files** tab.
12. ☐ Select **Open in Sharepoint**
13. ☐ In the Mark 9 Project Team library, click the **New** button, then click on **Word document**.
14. ☐ Click on **Sensitivity** in the ribbon and verify that **Mark 9 confidential** has been applied by default to this content – as it was created within a Team where that label was applied.
15. ☐ Close the **Document** tab in Edge, and then close the **Mark 9 Project Team – General** tab in Edge.

Exercise 2: Communication Compliance

Communication Compliance policies in Microsoft 365 allow you to capture employee communications for examination by designated reviewers. You can define specific policies that capture internal and external email, Microsoft Teams, or 3rd-party communications in your organization. Reviewers can then examine the messages to make sure that they are compliant with your organization's message standards and resolve them with classification type.

As more of Contoso's communication and collaboration shifts to Teams, it will become important for you to monitor that communication to ensure compliance with your organization's standards. To begin, you will need to establish a policy to monitor communications regarding the new Mark 9 prototype at Contoso.

Create a custom sensitive info type for the Mark 9 project

1. ☐ Select the **Information protection** tab in Microsoft Edge to switch back to the Microsoft 365 Compliance admin center.
2. ☐ In the left navigation of the Microsoft 365 Compliance admin center, select **Data classification**
3. ☐ On the Data classification page, select the **Sensitive info types** tab.
4. ☐ Click the **+ Create info type** button.
5. ☐ On the Choose a name and description pane, in the name box, type **Mark 9 Project Sensitive Info** and hit Enter.
6. ☐ Type **Dictionary of sensitive terms for Mark 9 project** in the Description box and hit Enter.
7. ☐ Click **Next**.
8. ☐ On the Requirements for matching pane, click **Add an element**.
9. ☐ Under Matching element, select the **Detect content containing** menu and choose **Keywords**
10. ☐ In the Keyword list text box enter **secret, prototype, flux, capacitor** and hit Enter.
11. ☐ On the Requirements for matching page – scroll down to review the settings and click **Next**.
12. ☐ On the Review and finalize pane, click **Finish**.
13. ☐ Review the Informational dialog and click **No** - we won't be testing the sensitive type in this guide.

Create a communication compliance policy

1. ☐ In the left navigation of the Microsoft 365 Compliance admin center under Solutions select **Communication Compliance**.
2. ☐ On the Communication compliance page, click the **+ Create Policy** button and select **Monitor for sensitive info** from the dropdown menu.
3. ☐ On the Monitor communication for sensitive information pane, click to place focus in the Policy name text box and then type **Mark 9 policy** and hit Enter.

4. ☐ In the Users or groups to supervise box, type **Mark** and select the **Mark 9 Project Team** from the resolved names list.
5. ☐ Click to place focus in the **Reviewers** field, then type **Meg** and hit Enter.
6. ☐ Select **Megan Bowen** from the list of suggested users.
7. ☐ Scroll down and select **Add sensitive info**.
8. ☐ On the Sensitive info types panel, scroll down through the list of available types to find and select **Mark 9 Project Sensitive Info** then click the **Add** button.
9. ☐ Click the **Create policy** button and then close the Your policy was created panel.

To learn more about communication compliance policies in Microsoft Teams, click here.

Exercise 3: Create a new DLP policy

Data Loss Prevention in Teams chat and conversations enables you to detect, automatically protect, and screen for sensitive information in chats and channel conversations. By creating DLP policies, admins can help prevent sensitive information from unintentionally being shared or leaked—either inside or outside of the organization. Files in Microsoft Teams are protected by DLP policies applied to OneDrive and SharePoint.

1. ☐ In the in the left navigation of the Microsoft 365 Compliance admin center, under Solutions, select **Data loss prevention.**
2. ☐ On the Data loss prevention page, select **+ Create policy**.
3. ☐ On the Start with a template or create a custom policy panel, under Categories, select **Privacy**.
4. ☐ In the template list, select **General Data Protection Regulation (GDPR)**
5. ☐ Review the GDPR template description and then select **Next**.
6. ☐ On the Name your DLP policy page, review the default name and description and then select **Next**.
7. ☐ On the Choose locations to apply the policy page - review the default selections, noting that Teams chat and channel messages are included, and then select **Next**.
8. ☐ Under Define policy settings, confirm the **Review and customize default settings from the template** radio button is selected and then click Next.
9. ☐ On the Info to protect panel, under Detect when this content is shared from Microsoft 365, select **Only with people inside my organization** and click **Next**.
10. ☐ On the Protection actions panel, under Detect when a specific amount of info is being shared at one time, click to place focus in the At least field and change the value from 10 to 1 and hit Enter.
11. ☐ Under Send incident reports in email – select **Choose what to include in the report and who receives it**.
12. ☐ On the Customize the incident report panel, select **Add or remove people**.
13. ☐ On the Add or remove people pane, select the checkbox next to **MOD Administrator**
14. ☐ Click to place focus in the search field, then type **meg** and hit enter.

15. ☐ Select the checkbox next to **Megan Bowen** and then click the **Add** button.
16. ☐ Click the **Save** button on the Customize the incident report panel.
17. ☐ Click the **Next** button on the Protection actions page.
18. ☐ On the Customize access and override settings panel, under Block these people from accessing Sharepoint, OneDrive and Teams content, select **Everyone Only the content owner, the last modifier and the site admin will continue to have access** and then scroll down to click the **Next** button.
19. ☐ On the Test or turn on the policy page, leave the radio button selected for **I'd like to test it out first** and check the box to **Show policy tips while in test mode.**
20. ☐ Click the **Next** button.
21. ☐ Review the policy settings and click the **Submit** button, then click **Done** to close the New policy created panel.

Exercise 4: Establish an Information barrier policy

Information barriers are policies that an admin can configure to prevent individuals or groups from communicating with each other. This is useful if, for example, one department is handling information that should not be shared with other departments. As an Administrator, you can create these policies using the Security & Compliance Center PowerShell cmdlets.

Note: To define or edit information barrier policies, you must be assigned an appropriate role, such as one of the following:

- Microsoft 365 Enterprise Global Administrator
- Office 365 Global Administrator
- Compliance Administrator
- IB Compliance Management

Your account is currently assigned to the Global Administrator role, so no additional action is needed.

Enable scoped search and then save the changes to Teams settings

Before you define your organization's first information barrier policy, you must enable scoped directory search in Microsoft Teams.

1. ☐ Switch to the Microsoft 365 admin center tab in Edge.
2. ☐ In the left navigation, under Admin centers, select **Teams**.
3. ☐ In the Microsoft Teams admin center, in the left navigation, select **Org-wide settings > Teams settings**.
4. ☐ In Teams settings, scroll down and under **Search by name, to the right of Scope directory search using an Exchange address book policy** select the toggle switch and verify it is set to **On**.

5. ☐ At the bottom of the page, select **Save** button.

Provide admin consent for information barriers in Microsoft Teams

Use the following procedure to enable information barrier policies to work as expected in Microsoft Teams.

1. ☐ Click the Windows PowerShell icon in the Windows Taskbar to switch back to PowerShell (Admin).
2. ☐ Type the following command and hit Enter:
   ```
   Connect-AzAccount
   ```

   Note: in this exercise you will be using the Az Powershell module. To learn more about the Az module functionality and how to install it, click here.

3. ☐ Log in with your administrator credentials:
   - Type admin@contoso.com and hit enter or click the **Next** button.
   - Type password and hit enter or click the **Sign in** button
4. ☐ Store the app ID for the Information Barrier Processor as a variable by entering the following command:
   ```
   $appId = "bcf62038-e005-436d-b970-2a472f8c1982"
   ```
5. ☐ Attempt to get the service principal for Information Barrier Processor:
   ```
   $sp = Get-AzADServicePrincipal -ApplicationId $appId
   ```
6. ☐ Type the following to check if the service principal exists and if not, create one for Information Barrier Processor :
   ```
   If ($sp -eq $null) { New-AzADServicePrincipal -ApplicationId $appId }
   ```
7. ☐ The the following to launch the admin consent flow:
   ```
   Start-Process
   "https://login.microsoftonline.com/common/adminconsent?client_id=$appId"
   ```
8. ☐ In the Permissions Requested dialog, review the information and then click the **Accept** button.
9. ☐ Confirm that the flow has completed and click the Windows PowerShell icon in the Windows Taskbar.

Define information barrier segments

Defining segments does not affect users; it just sets the stage for information barrier policies to be defined and then applied. You will need to define a segment for the Finance and Engineering departments respectively - based on the Department attribute on the user.

1. ☐ In PowerShell, enter the following and then press Enter to define the Finance segment for your organization:
   ```
   New-OrganizationSegment -Name "Finance"-UserGroupFilter "Department -eq
   'Finance'"
   ```

2. ☐ Briefly review the output, then scroll down and enter the following command to define the Engineering segment for your organization:
   `New-OrganizationSegment -Name "Engineering" -UserGroupFilter "Department -eq 'Engineering'"`
3. ☐ Review the organization segments. In Windows PowerShell, enter the following and then press Enter:
   `Get-OrganizationSegment | fl Name`

Define an information barrier policy

Contoso must keep their Finance department from communicating directly with Engineering. To do so you will define two policies, one blocking communication from Finance to Engineering and the other blocking the other direction of communication.

1. ☐ In Windows PowerShell, enter the following and then press Enter:
   `New-InformationBarrierPolicy -Name "Finance-Engineering" -AssignedSegment "Finance" -SegmentsBlocked "Engineering"`
2. ☐ Review the output of the command, then scroll down and enter the following command:
   `New-InformationBarrierPolicy -Name "Engineering-Finance" -AssignedSegment "Engineering" -SegmentsBlocked "Finance"`
3. ☐ Review the output of the command and then scroll down.

Apply the information barrier policies

Information barrier policies are not in effect until you set them to active status, and then apply the policies.

1. ☐ Review the existing information barrier policies. In Windows PowerShell, enter the following and then press Enter to confirm the names of your policies:
   `Get-InformationBarrierPolicy`
2. ☐ In Windows PowerShell, activate the Finance-Engineering policy by entering the following and then press Enter:
   `Set-InformationBarrierPolicy -Identity "Finance-Engineering" -State Active`
3. ☐ In Windows PowerShell, activate the Engineering-Finance by entering the following and then press Enter:
   `Set-InformationBarrierPolicy -Identity "Engineering-Finance" -State Active`
4. ☐ Start the policies by entering the following and then press Enter (running the command on one policy will start both of them):
   `Start-InformationBarrierPoliciesApplication -Identity "Finance-Engineering"`

To learn more about information barriers in Microsoft Teams, click here