

- Create a DLP policy with custom settings

In this exercise you will create a Data Loss Prevention policy in the Security & Compliance Center to protect sensitive data from being shared by users.

Perform the following steps



1. From the address bar in your browser you would have already typed `portal.office.com`, signed in and selected the Admin Icon for Microsoft 365 Admin Center.



2. From the Microsoft 365 Admin Center, click on Security, then click on the link **Office 365 Security and Compliance Center** in the right pane.



3. In the Security & Compliance Center select **Data loss prevention** from the left pane and click on **Policy**.



4. Click on (+) **Create a policy** to open the wizard for creating a new data loss prevention policy.



5. On the template screen, make sure **Custom** and **Custom policy are selected**. Click **Next**.



6. Type **IP Address DLP Policy** (look on the page for the blinking cursor then type the name) in the **Name** field (press Enter) and type **Protect IP addresses from being shared** to the **Description** field (press Enter). Click **Next**.



7. On the next screen make sure **Protect content in Exchange email, Teams chats and channel messages and OneDrive and Sharepoint documents** is selected and click

Next.



8. On the Policy settings page, make sure the option **Find content that contains:** is selected.



9. Click on **Edit** to add sensitive data types.



10. Click on **Add** and select **Sensitive info types**.



11. Click on (+) **Add** again.



12. Type into the search field **Address** and wait till the search results are displayed.



13. Select **IP Address** from the Sensitive information types.



14. Click **Add** and **Done** on the next screen.



15. Check the box on top of the page and make sure, **Any of these** is selected.



16. Click on **Save**.



17. Check if the **Detect when this content is shared:** box is selected.



18. Select **only with people inside my organization** from the dropdown list.



19. The sensitive information types have now been added. Click **Next**.



20. On the next screen, check that **Detect when content that's being shared contains** is selected.



21. Change the number from **10** instances of the same sensitive info type to **2** and click **Next**.



22. On the **Customize access and override permissions** page select **Next**.



23. Turn the policy on by selecting **Yes, turn it on right away**.



24. Click **Next**.



25. Check the configuration on the Review your settings page again and click **Create**.

You have now created a DLP policy that informs your users, if they want to share content that contains IP addresses.