**Create a DLP Policy using Power Automate**

For security reasons, administrators oftentimes want to ensure that certain data is kept protected. Power Platform allows you to create data loss prevention policies that define which connectors can share specific business data. For example, you may not want business data that is stored in SharePoint to be automatically published to its Twitter feed by a Power Automate flow.

Within Power Automate, you can define connectors for a flow that can be in two data groups – **Business data only** and **No business data allowed**. For a flow to run, all its connectors must be in one group or the other. If your flow has connectors in both groups, then the flow will automatically be suspended and will not run. By default, all connectors are assigned to the **No business data allowed** group. Therefore, if you want to include any data in your flow, you must add all the connectors used in the flow into the Business data only group.

### Task 1: Create a data loss prevention policy

In this task, Holly wants to create a data lost prevention policy for the flows that she plans to create as part of her pilot project. In this task, she will initially add the **SharePoint** connector to **Business data only** group. She will then see how this affects the flow that she just created.

1. You should still have the browser tab open to the **Manage your flows | Microsoft Power Automate** tab, which should still be displaying the **Flows** window and the **Team flows** tab. If not, then repeat the steps you performed in the prior task to get to this tab (from **Power Automate studio**, select **My flows**, and then select the **Team flows** tab.
2. In the top right corner of the screen, select the **gear (Settings)** icon, and then in the **Settings** pane that appears select **Admin Center**.
3. A new tab will open in your browser that displays the **Microsoft Flow Admin Center**. In the left-hand navigation pane select **Data policies**.
4. In the top right-side of the screen, select **+New Policy**.  
   ‎  
   ‎**Note:** If the window that appears is partially hidden by the left-hand navigation pane, select the icon that appears at the top of the navigation pane (the three lines stacked on top of each other). This contracts the pane and only displays the navigation icons. In doing so, the entire **Data Policy Name** window will appear. If you select the icon at the top of the navigation pane again, the window will still appear properly, and the navigation pane will display the text for each icon.
5. In the **Data Policy Name** window, the **Environments** tab is displayed by default. Under the **Choose environments** section, the **Apply to All environments** option is selected by default. Leave this option selected, and then select **Continue**. This will display the **Data Groups** tab in this window.
6. In the **Data Groups** tab, under the **Business data only** section, select **Add**.
7. In the **Add Connectors** window that appears, enter **Share** in the **Search connectors** field and then select **SharePoint** from the list of connectors with **Share** in its name. Select **Add connectors**.
8. This returns you to the **Data Policy Name** window, and **SharePoint** now appears in the **Business data only** group.  
   ‎  
   ‎Select **Save Policy**, which appears in the upper right corner of the screen. This returns you to the **Data loss prevention policies** window, which displays the policy that you just created.  
   ‎  
   ‎**Important:** You have created a data policy that has one of the two connectors used in your flow (SharePoint) in the **Business data only** group. However, Holly has forgotten that she actually has two connectors in her flow; the second connector is **Office 365 Outlook**, which manages the email that is automatically created and sent by the flow. This connector remains in the **No business data allowed** **(default)** group.  
   ‎  
   ‎In practice, you would not implement this policy as you need both connectors used by the flow in the same group. Continue on to see how connectors in both groups impact the flow.
9. In your browser, select the **Manage your flows | Microsoft Power Automate** tab to return to the **Flows** window that displays your flow in the **Team flows** tab.
10. Select the **Service Request Flow for new/modified tickets**, which displays the detail information about the selected flow.  
    ‎  
    ‎Note that the Status of the flow is **On**. Eventually, once the policy propagates through the system, the status will change from **On** to **Suspended**.  
    ‎  
    ‎**Important:** It can take several minutes for the policy to propagate; in testing, it has been found to take approximately 5 minutes. After that time, select the **Refresh** icon that appears to the right of the address bar. In the **Details** section, notice the **Status** of the flow, which should change from **On** to **Suspended**.  
    ‎  
    ‎Do NOT proceed to the next step until the **Status** of the flow has changed to **Suspended**. You may need to refresh the window a few times until you see this status change.
11. Once the flow has been suspended, select **Edit i**n the menu bar at the top of the page.
12. In the window that is returned, you will see the actions for your flow. Select **Save**.  
    ‎  
    ‎A warning message is returned at the top of the page that says: **Your flow was updated, but it is currently suspended since it uses a combination of connectors that conflict with the company data loss prevention policies or billing restrictions**.  
    ‎  
    ‎**Important:** Since this flow was already created at the time the policy was established, Power Automate automatically suspended the flow, which, in effect, turned the flow **Off**. If you subsequently create a new entry or modify an existing entry in the SharePoint list after the flow has been suspended, the flow will not run.
13. At the top of the page, above the warning message, select the left arrow to return to the Detail page for the flow.
14. In the heading at the top of the page, **Flow > Service Request Flow for new/modified tickets**, select **Flow** to return to the list of flows.
15. Leave your browser and all its tabs open for the next task.

### Task 2: Edit your data loss prevention policy

Although you created the DLP policy using the Flow Admin Center, the policy applies to all applications and flows in the Adatum Corporation environment. As such, the policy would apply for any Power App that uses these connections.

Now that Holly has seen what happens when she creates a DLP policy that only includes the SharePoint connector, she realizes that she needs to update the policy to include both Outlook and SharePoint in the **Business data only** group. While this will allow her flow to work, it will also prevent any future flow or app from running if it uses SharePoint, Outlook, and any other connector, since the additional connector is not in the **Business data only** group. For example, if Holly creates a second flow that includes SharePoint, Outlook, and Twitter, this first flow would still work, but the second flow would not since Twitter is not included in the **Business data only** group for this policy.

In your role as Holly, you will update this DLP policy to include Outlook as an additional connector in the **Business data only** group.

1. You should still be logged into your Domain Controller VM (LON-DC1) as **ADATUM\Administrator** and a password of **Pa55w.rd**; if not, then do so now.
2. You should still have the browser tab open to the **Manage your flows | Microsoft Power Automate** tab, which should still be displaying the **Flows** window and the **Team flows** tab.  
   ‎  
   ‎In your browser, select the **Microsoft Flow Admin Center** tab, which should be displaying the **Data loss prevention policies** window. If you closed this tab at the end of the prior task, then in the **Manage your flows | Microsoft Power Automate** tab, select the gear **(Settings)** icon, select **Admin center** in the **Settings** pane, and then in the **Microsoft Flow Admin Center,** select **Data policies.**
3. In the **Data loss prevention policies** window, locate your policy in the list, and then select the **Pencil (Edit)** icon that appears to the far right of the screen for this policy.
4. You will basically repeat the same steps that you performed in the prior task when you assigned the SharePoint connector to the policy; however, this time you will assign **Office 365 Outlook**.  
   ‎  
   ‎Try and perform the steps from memory, up to the point of updating the policy and saving it. If you succeed, skip to step **9**.  
   ‎  
   ‎If you don’t remember the exact sequence of steps, or you simply wish to follow the list of steps, then perform the following steps below.
5. In the **Data Policy Name** window, the **Environments** tab is displayed by default. Under the **Choose environments** section, the **Apply to All environments** option is selected by default. Leave this option selected, and then select **Continue**. This will display the **Data Groups** tab in this window.
6. In the **Data Groups** tab, under the **Business data only** group, notice that **SharePoint** is the only connector in this group. You now want to add **Outlook**, so select **Add**.
7. In the **Add Connectors** window that appears, enter **Outlook** in the **Search** **connectors** field and then select **Office 365 Outlook** from the list of connectors with **Outlook** in its name. Select **Add connectors**.
8. This returns you to the **Data Policy Name** window, where **Office 365 Outlook** now appears in the **Business data only** group alongside **SharePoint**.  
   ‎  
   ‎Select **Save Policy**, which appears in the upper right corner of the screen. This returns you to the **Data loss prevention policies** window, which displays the policy that you just created.
9. In your browser, select the **Manage your flows | Microsoft Power Automate** tab to return back to the **Flows** window that displays your flow in the **Team flows** tab. Notice that under the **Modified** column, it still indicates **Activity suspended**.
10. Select **Service Request Flow for new/modified tickets** to see the detail information about the flow.  
    ‎  
    ‎**Important:** Note that the **Status** of the flow is **Suspended**. When you first created the DLP policy, Microsoft Flow automatically changed the status of the flow from **On** to **Suspended** when you saved the policy and Flow realized that one of the data connectors for the flow was not in the policy’s **Business data only** group. However, when you edit a policy and change the connectors in either group, Flow does not re-evaluate this change to existing flows; therefore, the status of this flow will not be automatically changed from **Suspended** to **On** even though the policy now has both **SharePoint** and **Outlook** in the **Business data only** group. Instead, you will have to manually turn the flow **On**, which you will do in the next step.  
    ‎  
    ‎**Note:** If you delete a DLP policy, Flow does not re-evaluate how this policy deletion affects existing flows. Therefore, had you deleted this policy rather than modify it, your suspended flow would remain suspended, and you would have to manually turn it **On**, just as you have to do following this policy change.
11. At the top of the **Flow > Service Request Flow for new/modified tickets** window, select **Turn on i**n the menu bar at the top of the page.  
    ‎  
    ‎This displays a message below the menu bar that says: **Your flow is off: Service Request Flow for new/modified tickets.** This message simply indicates the status of the flow prior to it being turned **On.**
12. Select the **Refresh** icon that appears to the right of the address bar. In the **Details** section, notice the **Status** of the flow, which should change from **Suspended** to **On**.
13. In your browser, close the **Power Automate** tabs, but leave the **SharePoint** tabs that are related to your **Service Desk Requests** list open for the next exercise.