



## Module 4

# Data Loss Prevention Policies

Microsoft Customer Success Unit



# CONDITIONS AND TERMS OF USE:

© Microsoft Corporation. All rights reserved.

You may use these training materials solely for your personal internal reference and non-commercial purposes. You may not distribute, transmit, resell or otherwise make these training materials available to any other person or party without express permission from Microsoft Corporation. URL's or other internet website references in the training materials may change without notice. Unless otherwise noted, any companies, organizations, domain names, e-mail addresses, people, places and events depicted in the training materials are for illustration only and are fictitious. No real association is intended or inferred. THESE TRAINING MATERIALS ARE PROVIDED "AS IS"; MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED IN THESE TRAINING MATERIALS.

# Introduction

In this lesson, you will learn the following:

- Understand Data Loss Prevention Policies.
- DLP Policies Scope.
- How to Create a DLP Policy.
- How to Manage a DLP Policy.



# Data Loss Prevention Policies

# Data Loss Prevention Policies

- Power Platform DLP policies allow you to control data flows across data connectors when used within Power Apps and Power Automate
- Simply put, DLP enables admins to isolate business data from personal use data within Power Platform
- Able to classify Power Platform connectors across business and non-business groups and additionally choose to block certain connectors
- As you see on the user interface here the DLP policy allows admins to segregate connectors across three different buckets – **Business**, **Non-business** and **Blocked**

DLP Policies > New Policy

✓ Policy name

● Connectors

○ Scope

○ Review







⚙ Set default group

Assign connectors ⓘ

Business (0) Non-business (465) | Default Blocked (0)

🔍 Search connectors

Connectors for non-sensitive data. Connectors in this group can't share data with connectors in other groups. Unassigned connectors will show up here by default.

	Name ↑		Blockable	Class
	10to8 Appointment S	:	Yes	Standard
	365 Training	:	Yes	Premium
	Act!	:	Yes	Standard
	Acumatica	:	Yes	Premium
	Adobe Creative Cloud	:	Yes	Premium

# Connectors Classification



## Business

A given Power App or Power Automate resource can use one or more connectors from Business group

If a Power App or Power Automate resource uses a **Business** connector, it cannot use any **Non-business** connector



## Non-business

A given Power App or Power Automate resource can use one or more connectors from **Non-business** group

If a Power App or Power Automate resource uses a **Non-business** connector, it cannot use any **Business** connector



## Blocked

Any Power App or Power Automate resource cannot use any connector from **Blocked** group

All Microsoft owned premium connectors and third-party connectors (standard and premium) can be blocked

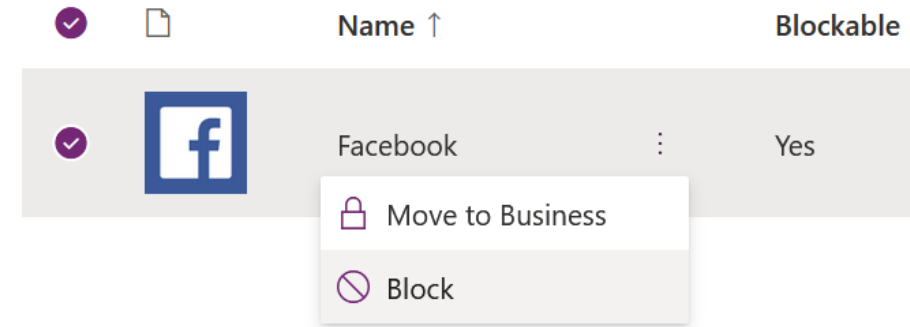
All Microsoft owned standard connectors and Microsoft Dataverse cannot be blocked

# How Data is Shared among Data Groups?

- Data **can't** be shared among connectors that are located in different groups.
- For example, if you place **SharePoint** and **Salesforce** connectors in the Business group and you place **Gmail** in the Non-Business group, makers can't create an app or flow that uses both the SharePoint and Gmail connectors.
- This in turn restricts data flows between these two services in Microsoft Power Platform.
- Although data can't be shared among services in different groups, it can be shared among services within a specific group.
- From the earlier example, because **SharePoint** and **Salesforce** were placed in the same data group, makers can create an app or flow that uses both SharePoint and Salesforce connectors together.
- This in turn allows data flows between these two services in Microsoft Power Platform.
- The key point is that connectors in the same group can share data in Microsoft Power Platform, whereas connectors in different groups can't share data.

# Blocked Data Group

- Data flow to a specific service can be blocked by marking that connector as **Blocked** which restricts all data flows to this service in Microsoft Power Platform.
- For example, if you place Facebook in the Blocked group, makers can't create an app or flow that uses the Facebook connector.
- All third-party and Microsoft-owned Premium (except Dataverse) connectors can be blocked.
- All connectors driving core Power Platform functionality like Dataverse and Approvals as well as connectors enabling core Office customization scenarios like Microsoft Enterprise Plan standard connectors will remain non-blockable to ensure core user scenarios remain fully functional.
- These non-blockable connectors can be classified into Business or Non-Business data groups.



## Assign connectors ⓘ

Business (0) Non-business (464) | Default **Blocked (1)**

Blocked connectors can't be used where this policy is applied.

		Name ↑	Blockable
		Facebook	Yes




# Custom Connector Classification

- At the moment custom connectors aren't part of the standard configuration capabilities of DLP policies in the **Power Platform admin center**.
- You have to use PowerShell commands to set and manage custom connectors in DLP policies PowerShell commands to set them up into Business, Non-Business, and Blocked groups.
- As custom connectors are **environment level** resources you can use them only in environment level policies
- By using PowerShell, you can configure DLP policy to include these connectors.


# Default Data Group for New Connectors

Following grouping logic is applied to new connectors added to Power Platform:




- Power Platform connector ecosystem keeps evolving and adding new connectors
- If connectors are added after DLP policy creation, admins have not had a chance to explicitly categorize them.
- These new connectors are automatically added to 'default connector' group identified for them
- Admins can set the 'default connector' group for new connectors in a DLP policy to – Business or Non-business or Blocked
- Admins can review these new connectors retrospectively and classify them explicitly as appropriate

 Set default group

### Assign connectors

Business (0)   **Non-business (465) | Default**   Blocked (0)    Search connectors

Connectors for non-sensitive data. Connectors in this group can't share data with connectors in other groups. Unassigned connectors will show up here by default.

	Name ↑		Blockable	Class
	10to8 Appointment S	:	Yes	Standard
	365 Training	:	Yes	Premium

#### Set default group

☐ Business  
Connectors for sensitive data.

☒ Non-business  
Connectors for non-sensitive data.

☐ Blocked  
Blocked connectors can't be used where this policy is applied. (Unblockable connectors will be in Non-business by default.)

Apply

Cancel

# Policy Scope

## Tenant policies have three scope settings

### All environments

By default, tenant level policies will be applied to all environments created in the tenant

### All except selected environments

Tenant admins can choose to exclude specific environments to apply the policy

### Only selected environments

Tenant admins can choose to include only specific environments to apply the policy

## Environment policies have one setting

### One environment only

Environment admins can choose to apply the policy on one environment at a time

### Define scope

Choose the environments to add to this policy. [Learn more](#)

**I want to:**

- ☒ Add all environments ⓘ
- ☐ Add multiple environments
- ☐ Exclude certain environments

Data policies		
Create and manage connector policies to protect data within your org (tenant). <a href="#">Learn</a>		
Name	Scope	Applied to
Test	Environment	Test

# View DLP Policies

Using the view policy feature, environment admins can view tenant-level policies and policies within environments that the admin has access to, at an individual policy level. Non-admins can also view tenant-level policies using this feature.

The screenshot displays the Power Platform admin center interface for 'Contoso Electronics'. The top navigation bar includes the logo, the name 'Contoso Electronics', and the path 'Power Platform admin center | Admin center'. On the right of the header are icons for settings, help, and a user profile labeled 'MA'. A left-hand navigation pane lists various sections: Environments, Analytics, Resources, Help + support, Data integration, Data (preview), Data policies (which is currently selected and highlighted with a purple bar), and Admin centers. The main content area is titled 'Data policies' and includes a '+ New Policy' button and a search bar. Below this, a descriptive text states: 'Create and manage connector policies to protect data within your org (tenant). [Learn more](#)'. A table follows, listing existing data policies with columns for Name, Scope, Applied to, Created by, Created, Modified by, and Modified. Two policies are shown: 'Contoso Restricted Development Po...' and 'Contoso Default Policy', both created on 11/18/2020 by the 'MOD Administrator'.

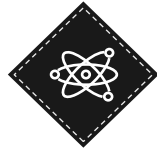
Name	Scope	Applied to	Created by	Created	Modified by	Modified
Contoso Restricted Development Po...	Org (tenant)	Contoso Production	MOD Administrator	11/18/2020	MOD Administra...	11/18/2020
Contoso Default Policy	Org (tenant)	All environments	MOD Administrator	11/18/2020	MOD Administra...	11/18/2020

# Combining DLP Policies Impact



## Blocked connectors

- If a connector is marked as 'blocked' in any one DLP policy applied to the environment, then the net outcome is that this connector is blocked from usage within the environment
- It doesn't matter if other DLP policies applied to the environment mark it as business or non-business



## Business/Non-Business connectors

If all DLP policies applied to the environment mark certain set of connectors as business or non-business, then the most **restrictive** groupings define what connectors can be used together vs. not

For example –

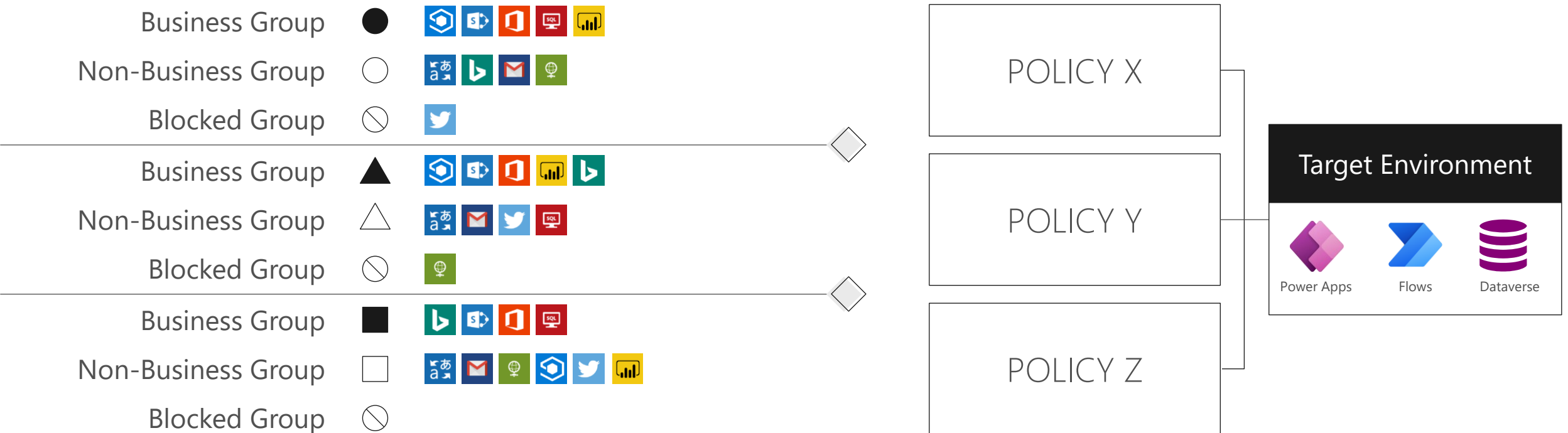
Policy X = B {1,2,3} NB {4,5} ; Policy Y = B {3,4,5} NB {1,2}

Then –

Net outcome : {1,2} {3} {4,5}

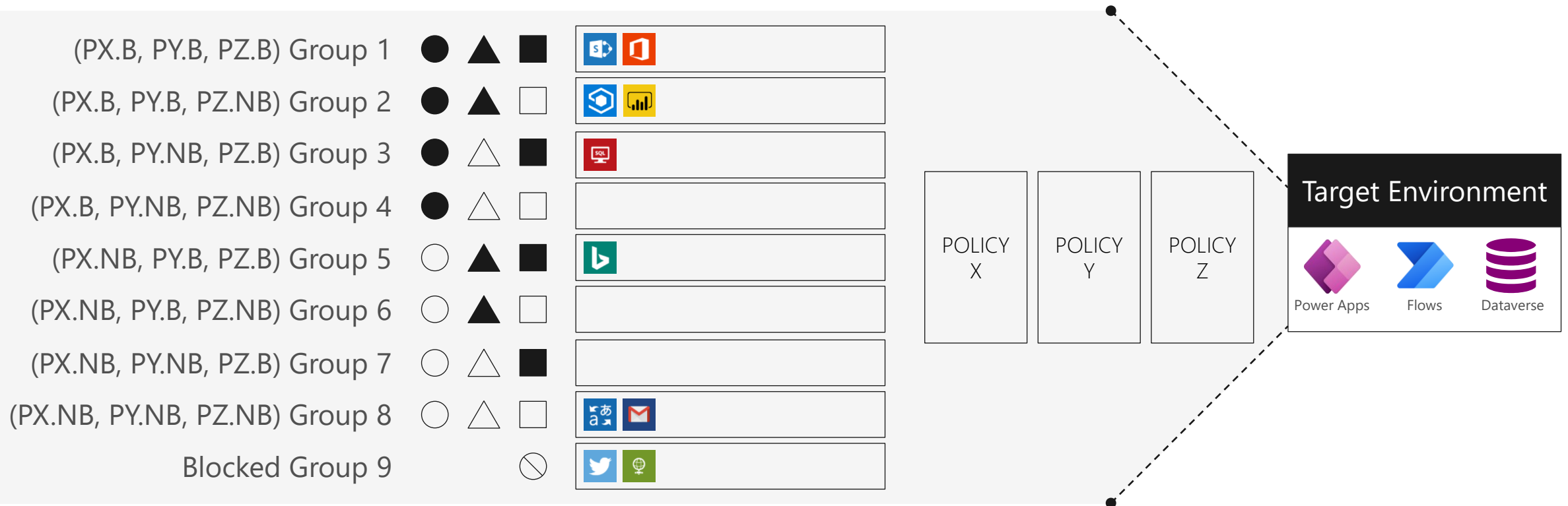


# Power Platform Multiple DLP Policy – Example Scenario



Multiple DLP policies applied to the same environment grouping connectors across Business/Non-business/Blocked. This set up makes the outcome of what connectors can be used together – Fragmented and hard to predict

# Power Platform Multiple DLP Policy – Net Outcome



All blocked connectors map to blocked. For business/non-business - 3 policies will fragment connector grouping outcome into as many as  $3^2 = 8$  different sets. For predictable outcomes use minimal number of DLP policies per environment

# DLP Policy Enforcement



## Design-time

Power Apps makers see an error upon using connectors that don't belong together or are blocked using DLP policies. Apps violating DLP policies cannot be saved at design time unless DLP violation is resolved.

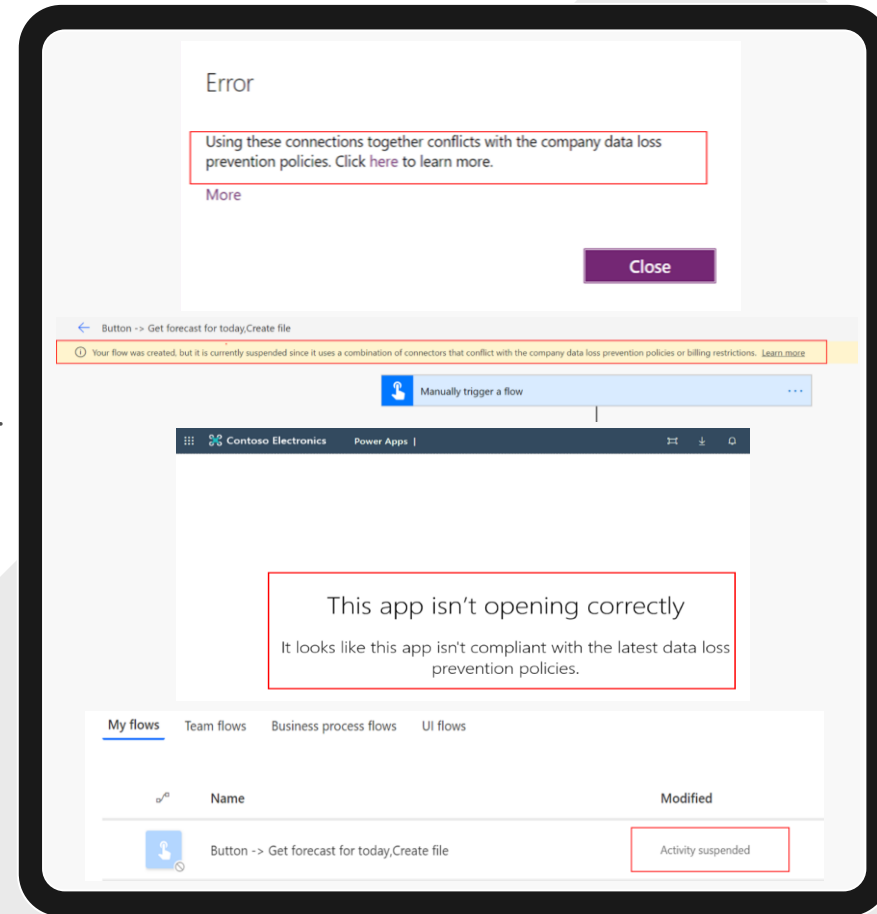
Power Automate makers see a warning while saving a flow using connectors that don't belong together or are blocked using DLP policies. Flow will be saved but marked as 'Suspended' and will not execute unless DLP violation is resolved.



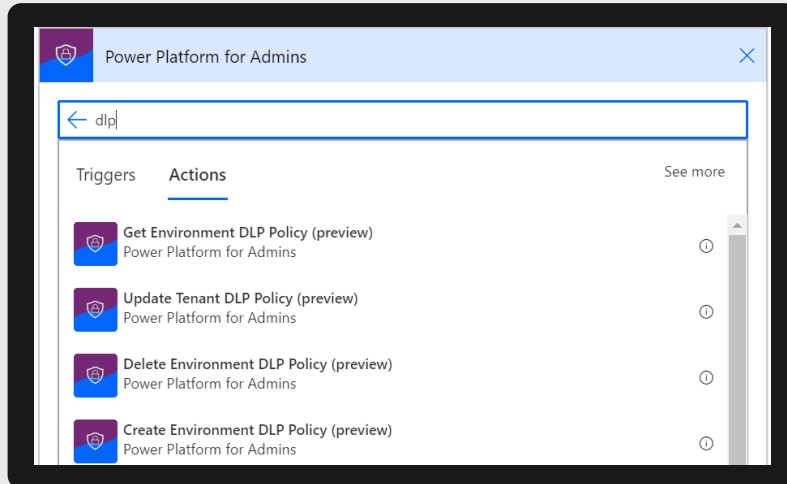
## Run-time

If DLP policy changes impact an existing Power App negatively and it becomes non-compliant then users are no longer able to launch it and get an error.

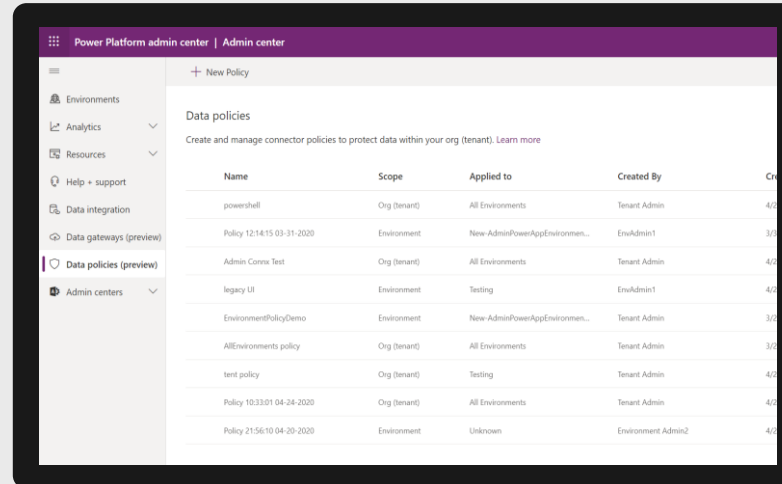
If DLP policy changes impact an existing Power Automate negatively and it becomes non-compliant then it is automatically marked as suspended. Users are no longer able to execute it. Power Automate suspension may take ~5 mins to come into effect after policy changes.



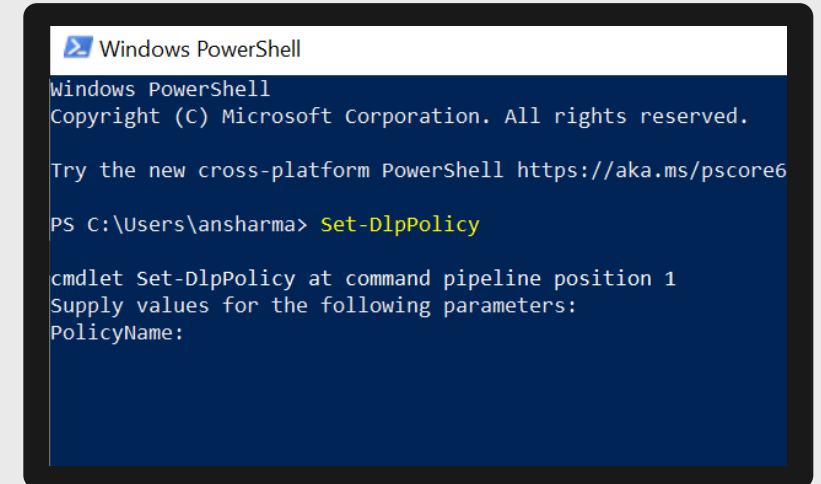
# DLP Management Interfaces



Power Platform for Admins  
Connector



Power Platform  
Admin Center



Power Apps  
PowerShell

# Labs: Module 4

1. Create DLP Policy Using UI
2. Create DLP Policy using PowerShell





