BLACK CELL
Protecting critical infrastructures

Compliance in Microsoft Purview Whitepaper

Table of Contents

1. Introduction 3

1.1. Information protection 3

1.2. Data life cycle management 3

1.3. Data loss prevention 4

2. Configuring a custom DLP policy 5

2.1. First steps 5

2.2. Choose the information to protect 6

2.3. Name your policy 7

2.4. Location to apply the policy 7

2.5. Policy settings 8

2.6. Advanced DLP rules 8

2.6.1. Conditions 8

2.6.2. Actions 9

2.6.3. User notifications 10

2.6.4. User overrides 10

2.6.5. Incident reports 11

2.7. Test or turn on the policy 11

2.8. After the test 12

3. Executive summary 12

4. References 12

1. Introduction

Microsoft Purview is a comprehensive set of data management solutions to govern, protect, and manage an organization's entire data estate. Among its many features the document introduces three with special focus on data loss prevention.

1.1. Information protection

Information protection is the process of safeguarding information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Information protection is important to preserve confidentiality, integrity, and availability. To achieve these goals, information protection employs security solutions like encryption and other technologies, as well as policies and processes.

Microsoft Purview Information Protection (formerly Microsoft Information Protection) provides the tools you need to discover, classify, and protect sensitive information by using labels and label policies. In essence you create a label and you set your conditions and restrictions on that label after assigning that label to a label policy, a group of users or group of devices.

1.2. Data life cycle management

Data management is a critical part of any software platform. Data is generated from many sources, such as business processes, network operations centres, mobile devices, social media sites, and other data-sharing environments. This data must be managed effectively to keep the customer safe and meet internal compliance requirements. Data lifecycle management (DLM) is a best practice approach that covers all stages of the data life cycle, from production to data destruction, data management, data protection, and data governance. By following DLM principles, businesses can establish that the correct data is at the place where it is supposed to be, enabling them to capitalize on data insights and create new opportunities. A more holistic view of data usage could then be gained by applying data science techniques through the various phases of the client's journey, allowing them to detect breaches or other potential misuse.

In Microsoft Purview Data lifecycle management, there are important tools like retention polices. The difference between backup and retention is that backup is used for operational and disaster recovery purposes, whereas retention is for compliance and legal reasons.

1.3. Data loss prevention:

Data is the key for information-based organizations nowadays. Have you ever wondered what would happen to your business if your data leaked? Your business could be destroyed. Amidst data breaches, cyberattacks, corporate espionage and data privacy regulations, data loss prevention (DLP) technologies have become an essential component of today's business.

DLP is a set of products, strategies, technologies, and techniques to prevent unauthorized access to sensitive data. The main causes of data loss are accidental deletion, data migration, accidental overwrite, external hackers or malware, and malicious network insiders.

Recently, the adoption of cloud-based SaaS applications, such as Microsoft 365 has increased. That's why continuously more data is being stored in the cloud. However, the cloud is not immune to data loss, therefore we need the best settings to keeping our data safe.

Organizations have sensitive files to handle. For instance, proprietary data, credit card numbers, health records, financial data, or social security numbers. How Microsoft deals with this obstacle? Microsoft Purview Data loss prevention is capable of preventing users from accidentally or intentionally sharing sensitive content, identify sensitive information (Exchange Online, SharePoint Online, OneDrive, Microsoft Teams, Windows devices), and monitor and protect confidential files (Excel, PowerPoint, Word and Outlook). Microsoft Purview has features like DLP alerts and reports which can be customized according to your company policies.

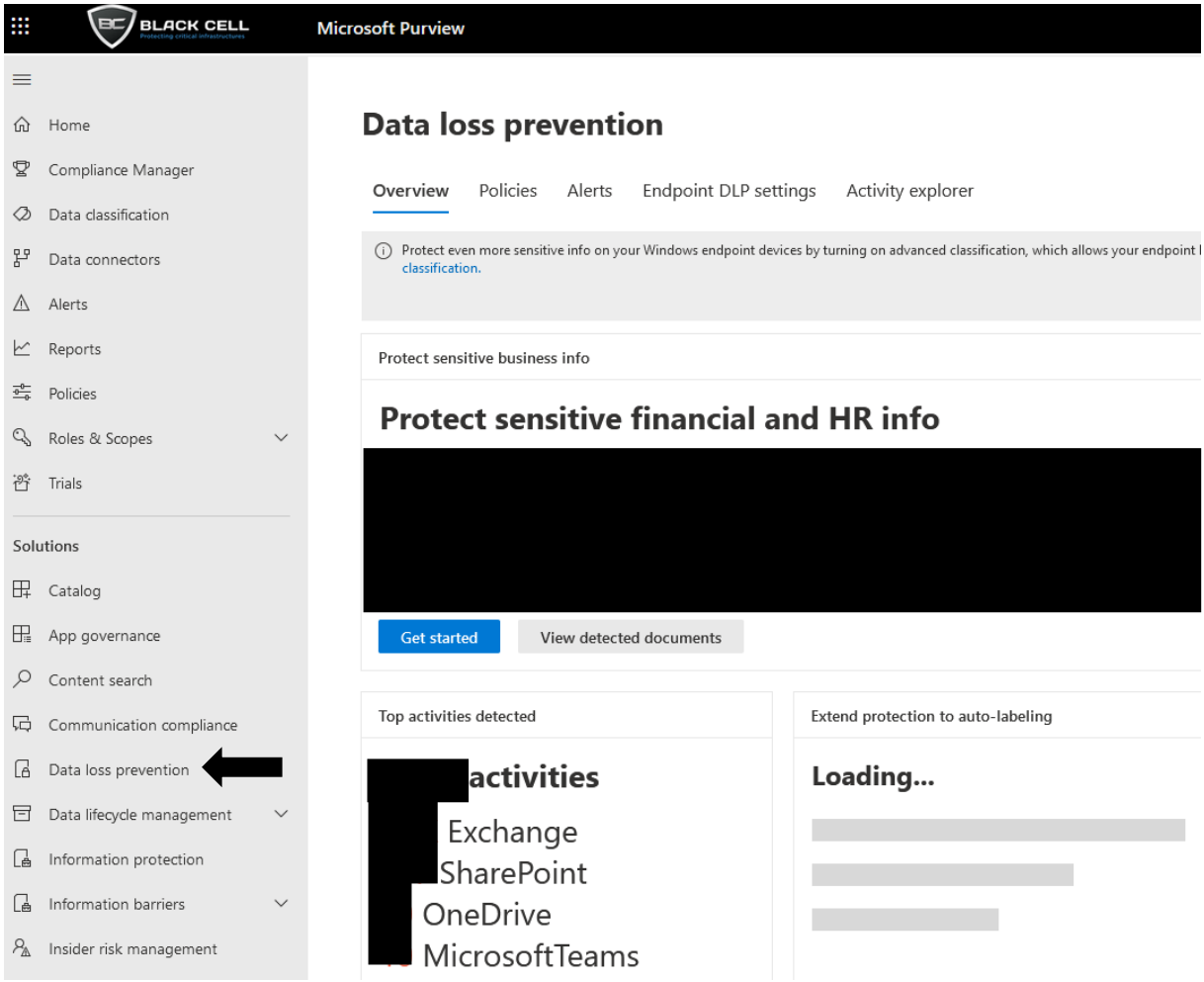
2. Configuring a custom DLP policy:

One of the most important aspects of security and compliance is data loss prevention. In the following section we are going to create an example policy that will prevent external users from accessing financial and tax related sensitive data.

2.1. First steps

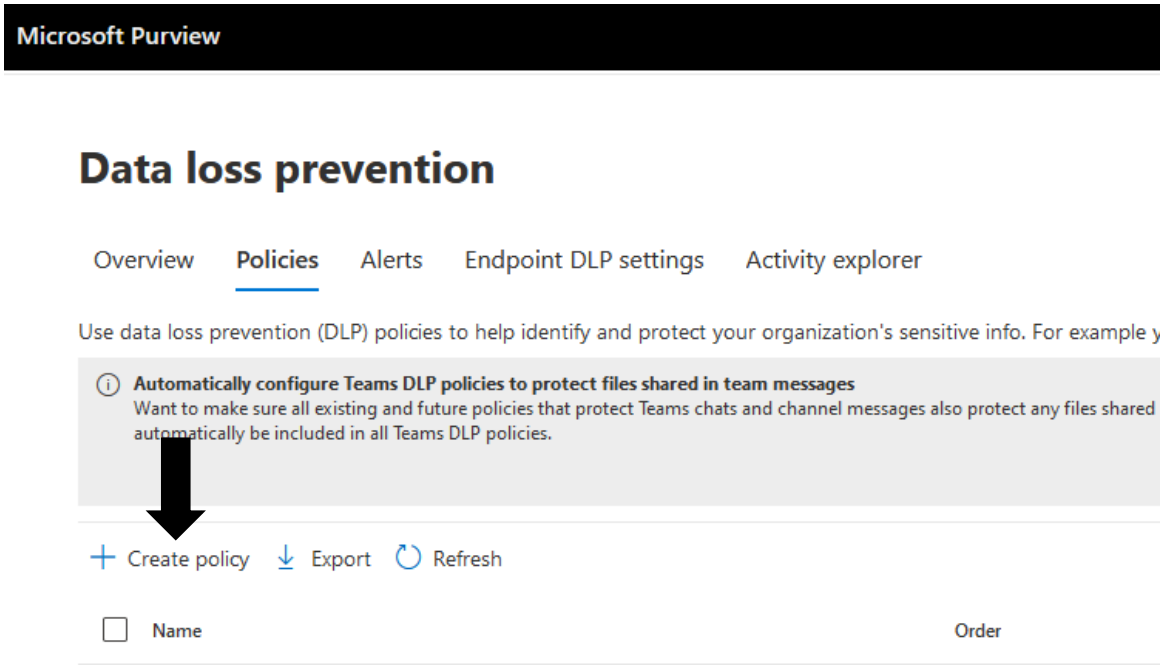
Log into Microsoft Purview on the following website: https://compliance.microsoft.com or on https://admin.microsoft.com, below *Admin centers* select *Compliance* blade.

On Microsoft Purview select Data loss prevention blade.



The *Overview* page gives us information about our organization data loss prevention, such as *Top activities detected* on OneDrive, SharePoint, OneDrive, and Microsoft Teams.

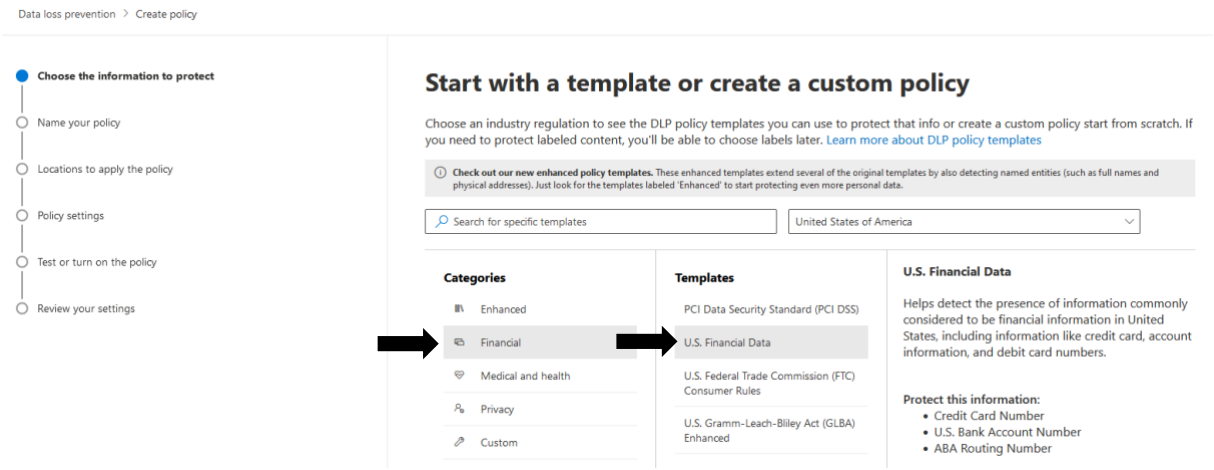
To define a new policy, click *Policies* and then *Create policy* in the menu at the top.



2.2. Choose the information to protect

Policies can be created by choosing a basic template which can be modified easily or by creating our own custom policy.

In this tutorial, select *Financial* category and from the template list U.S Financial Data.

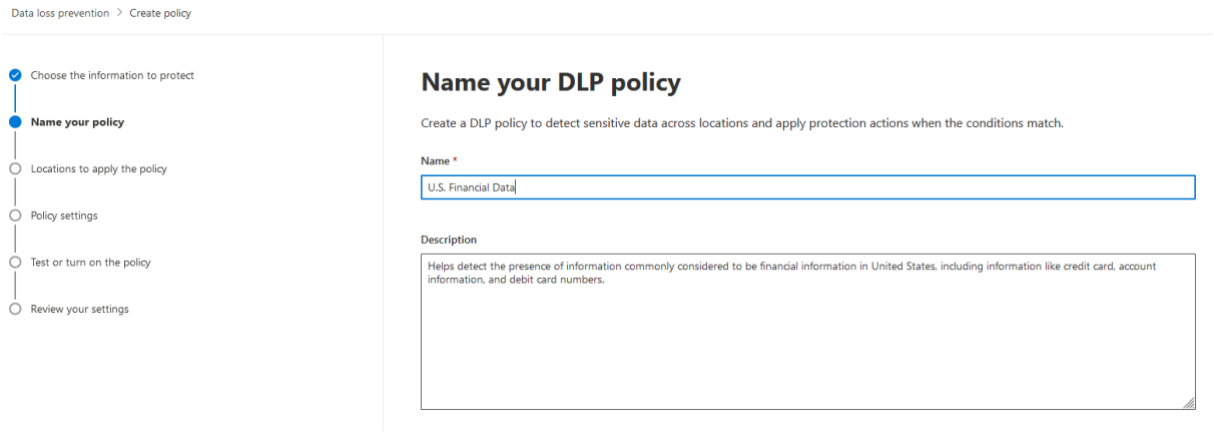


More details about DLP policy templates can be found under the following link: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide

Click Next.

2.3. Name your policy

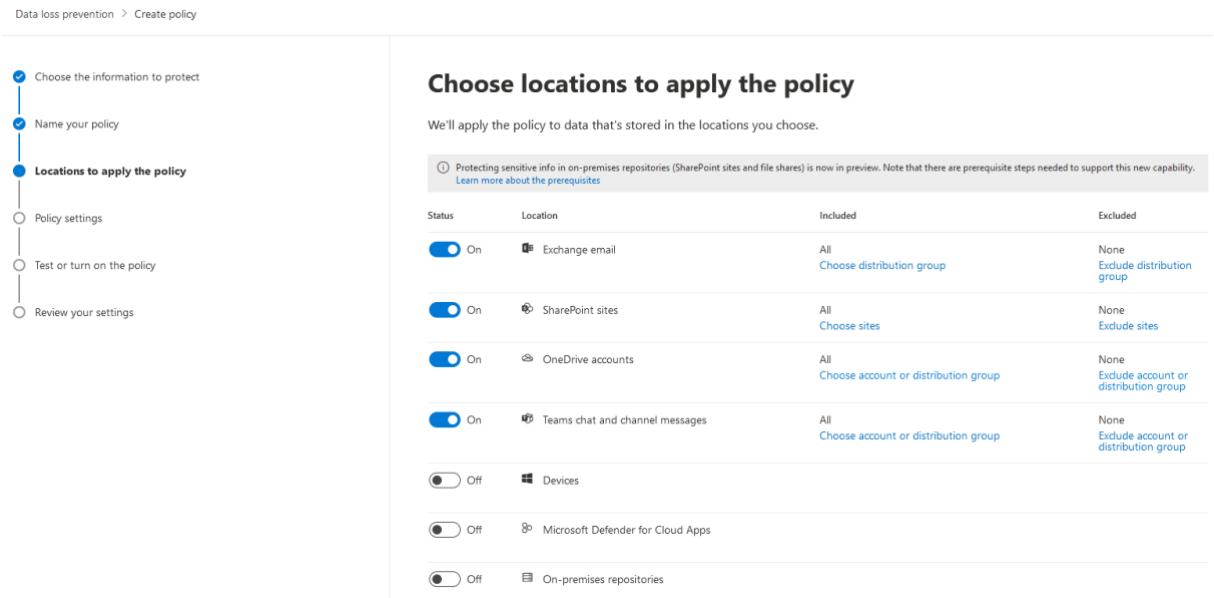
Provide a name for the policy. A detailed description is highly recommended.



Click Next.

2.4. Location to apply the policy

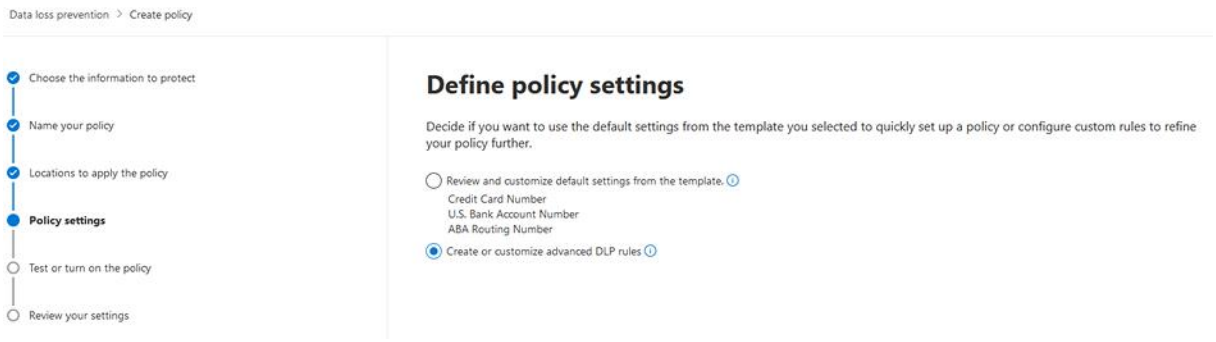
Choose the Location to apply the policy to. By default, everything will be selected, and groups or users can be excluded. The purpose here is to select the locations with the highest risk such as Exchange email, SharePoint sites, OneDrive, etc.



Click Next.

2.5. Policy settings

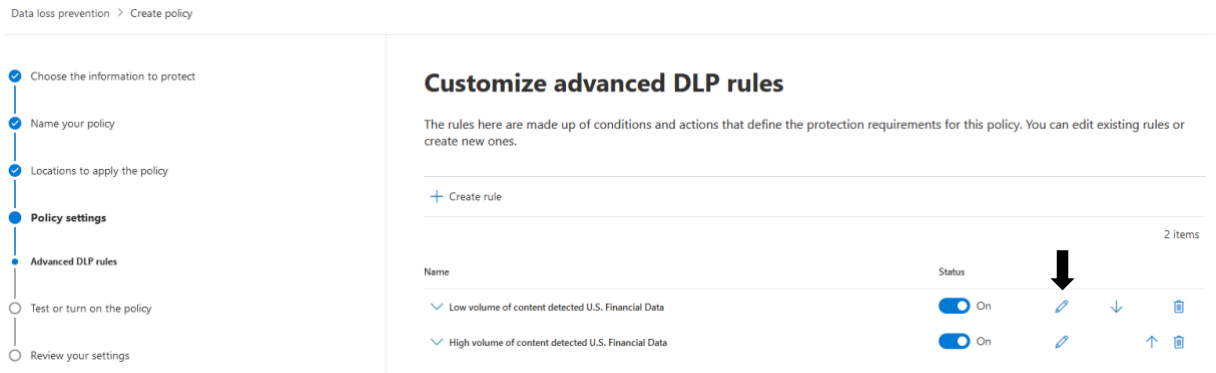
At this step, the default settings from the template are displayed. Select *Create or customize advanced DLP rules*, where rules can be added to the policies.



Click Next.

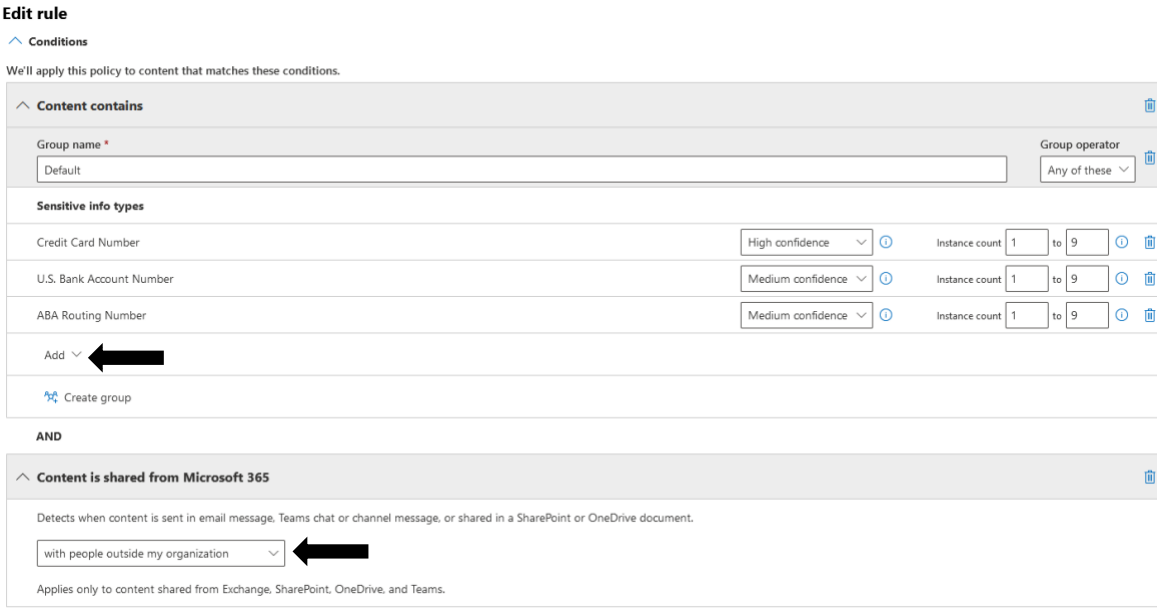
2.6. Advanced DLP rules

From the list choose Low volume content detected U.S Financial Data and click on pencil icon to edit the DLP rule.

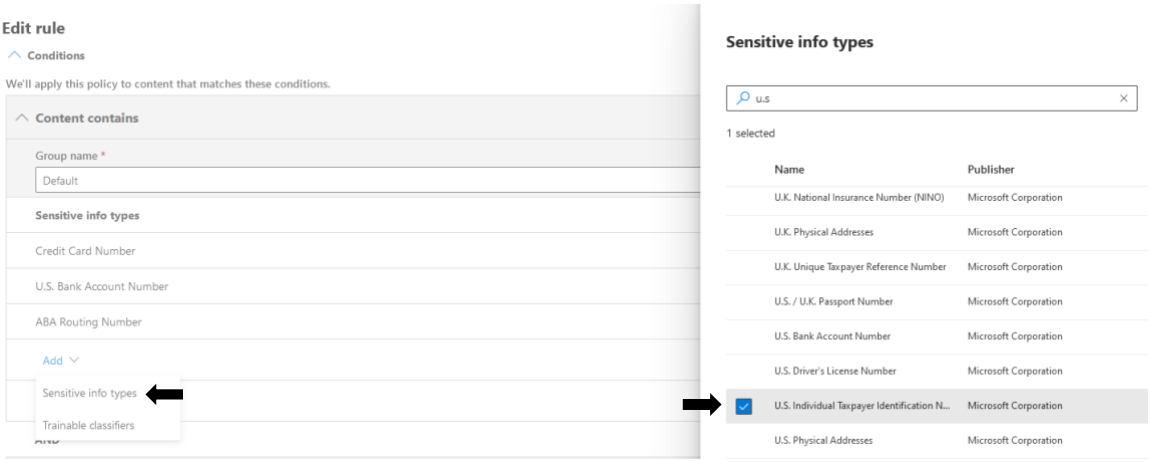


2.6.1. Conditions

In section *Content is shared from Microsoft 365,* choose the option *with people outside my organization*. This condition will affect users outside of the organization. More sensitive information types can be added with the confidence level selected. Click *Add*.



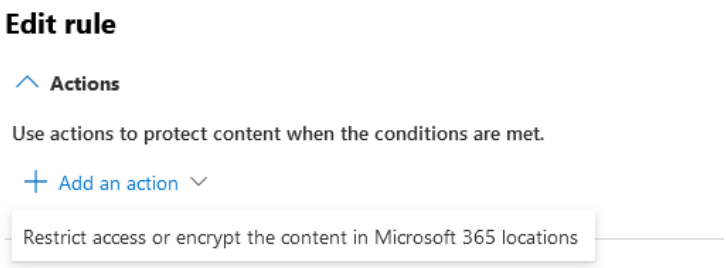
Choose sensitive info types, scroll down, and pick out U.S. Individual Taxpayer Identification Number (ITIN).



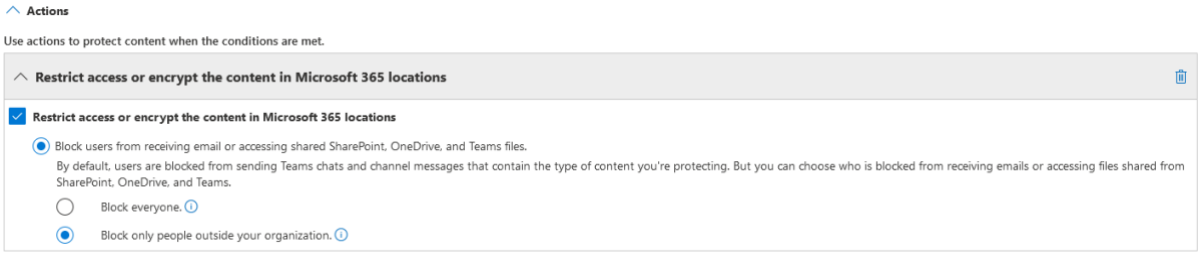
Click Add.

2.6.2. Actions

Click *Add an action* and choose *Restrict access or encrypt the content in Microsoft 365 location*.

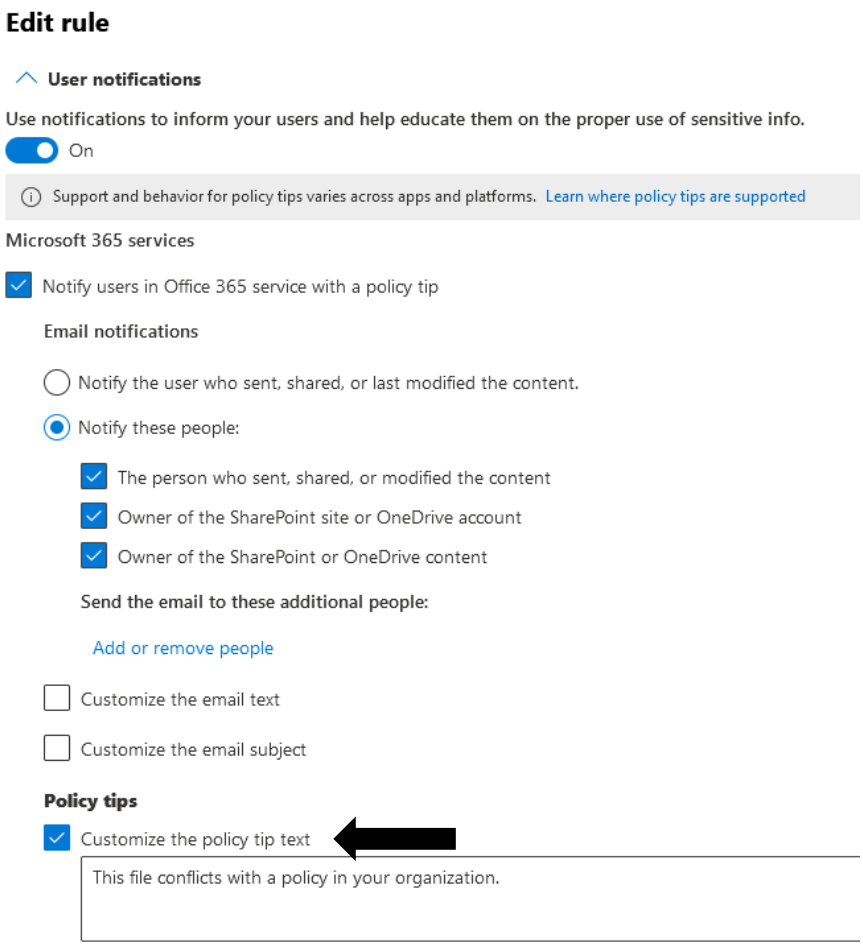


Apply this action only people outside your organization.



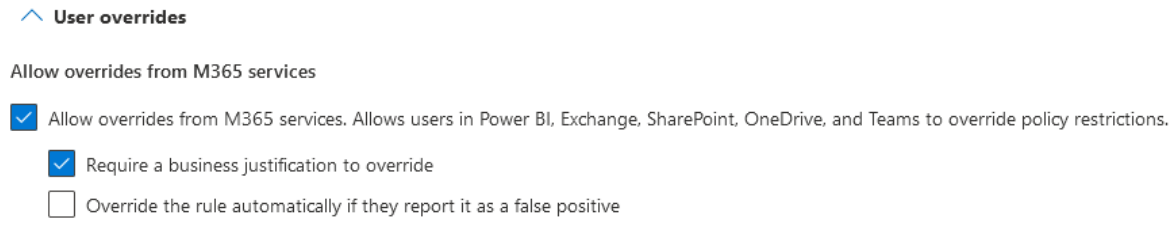
2.6.3. User notifications

In this section, how to notify the users about an action was taken can be defined. Under *Policy tips*, check the box next to *Customize the policy tip text*. If a file contains Personally Identifiable Information (PII) a notification will be sent to the user in a pop-up window. These notifications help to keep users informed and educated about organization's DLP policies.



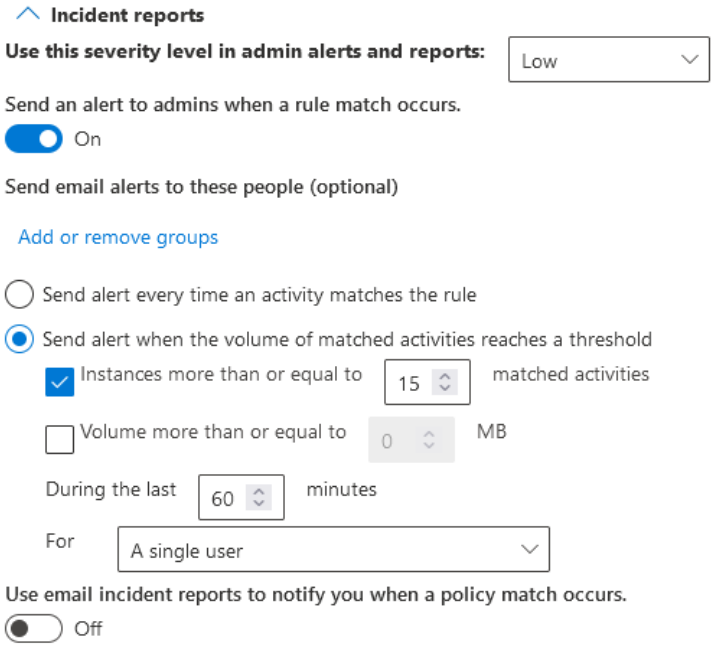
2.6.4. User overrides

Choose *Require a business justification to override* to mandate users to provide a rationale for deviating from the policy rule. For example, a salesperson may be allowed to override this policy with a proper business justification.



2.6.5. Incident reports

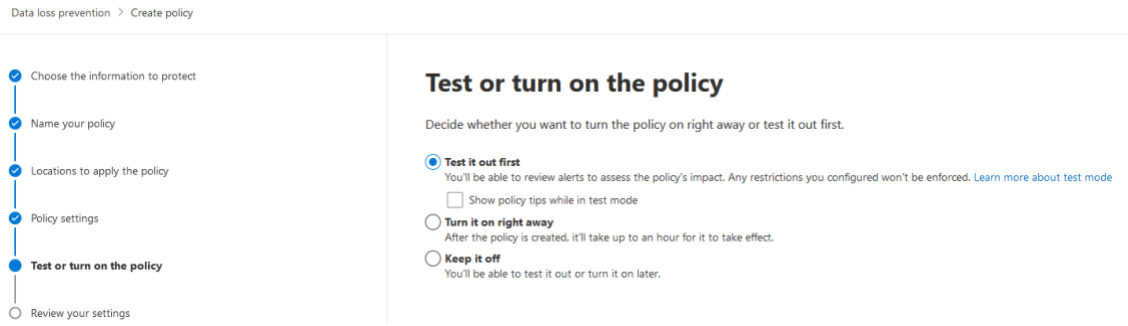
Various options are available for generating reports on policy rule matches. An alert to an admin or to any optional groups of users can be sent if a rule match occurred. Number of alerts can be limited based on customizable thresholds. The priority of the alert can be set.



Click save and next.

2.7. Test or turn on the policy

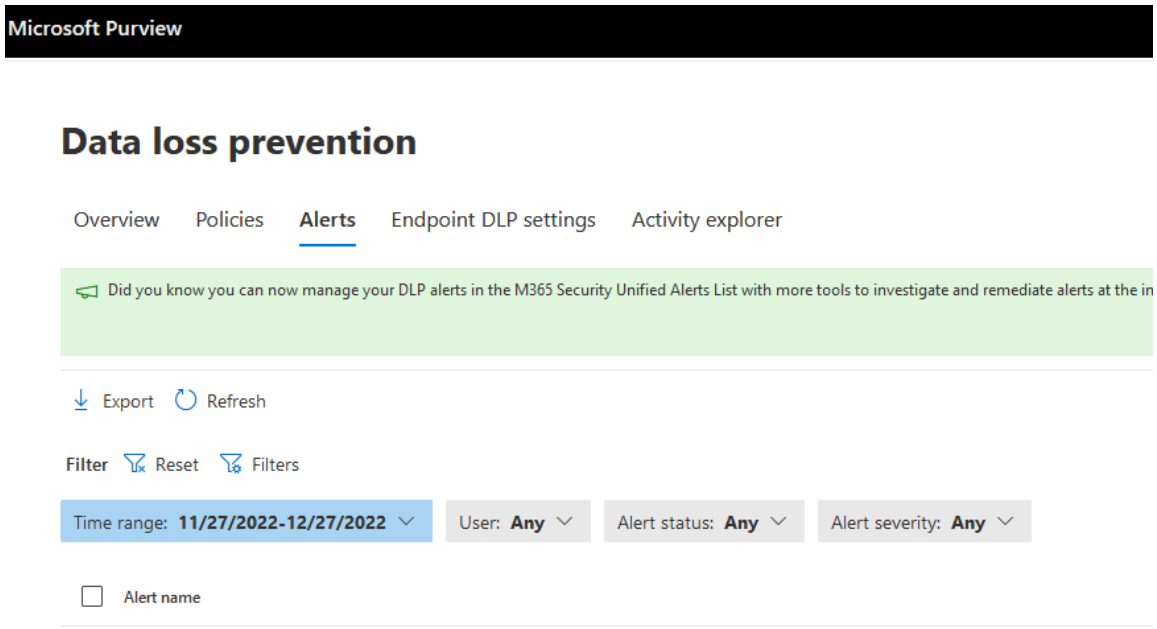
It is recommended that you test the policy first to make sure that it is set up correctly.



Click Next. Review your settings and select Submit.

2.8. After the test

If everything went fine and the policy is active, under the *Data loss prevention* blade, *Alerts* tab or *Activity explorer* can be checked to see if the policy generated any alerts.



3. Executive summary

Microsoft Purview provides numerous opportunities to keep our data safe. These options are essential for organisations to protect against hackers and malicious actors. The Data loss prevention feature enables high level of customization for setting rules in the data protection policies and can play a vital role in the organization's data lifecycle management.

4. References

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

https://azure.microsoft.com/en-gb/products/purview/