Filename: microsoft-ms101-9-1-1-what-is-data-loss-prevention-and-how-does-it-work
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Configure Data Loss Prevention (DLP)
EpisodeName: What Is Data Loss Prevention (DLP) & How Does It Work?
Description: Adam and Wes overview what Data Loss Prevention (DLP) is and how it works.

What Is Data Loss Prevention (DLP) & How Does It Work?

Manage Microsoft 365 Governance and Compliance (35-40%)

Configure Data Loss Prevention (DLP)
• Configure DLP Policies
• Design Data Retention Policies in Microsoft 365
• Manage DLP Exceptions
• Monitor DLP Policy Matches
• Manage DLP Policy Matches

==========

What is Data Loss Prevention (DLP) & How Does It Work?

NOTE: you should expect to be asked about how to CREATE, CONFIGURE & MANAGE DLP Policies (emphasis on configuration) on the exam !!!

DLP is designed to help prevent the leakage of sensitive information/data. It is integrated with Exchange, Outlook, SharePoint, OneDrive and Teams. It also can protect data in the desktop versions of Excel, PowerPoint and Word.

DLP relies on content analysis to scan information flows and detect information that has been labeled as sensitive. Content analysis methods include:

```
• Dictionary Matches
• Keyword Matches
• Regular Expression Matches
• Internal Functions (func_expiration_date)
```

NOTE: There are NO DEFAULT DLP Policies. Once policies are created, they must be synched across the multiple technologies that use them.

What does Policy Synch look like?

```
1. New policy is created in O365 Security & Compliance Center
2. Policy is synched to the central policy store
3. Policy is synched from central policy store to ALL technologies
4. Synch completes and then evaluation of content based on the policy starts
```

NOTE: DLP policies created in O365 Security & Compliance & DLP policies created in the Exchange Admin Center can co-exist and work side by side.

Rules created in the Exchange admin center take precedence.

All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

This means that:

Messages that are blocked by Exchange mail flow rules will not get scanned by DLP rules created in the Security & Compliance Center.

If an Exchange mail flow rule modifies a message in a way that causes it to match a DLP policy in the Security & Compliance Center - such as adding external users - then the DLP rules will detect this and enforce the policy as needed.

Also note that Exchange mail flow rules that use the "stop processing" action do not affect the processing of DLP rules in the Security & Compliance Center - they will still be processed.

Policy tips in the Security & Compliance Center vs. the Exchange admin center:

Policy tips can work either with DLP policies and mail flow rules created in the Exchange admin center, or with DLP policies created in the Security & Compliance Center, but not both.

This is because these policies are stored in different locations, but policy tips can draw only from a single location.

If you have configured policy tips in the Exchange admin center, any policy tips that you configure in the Security & Compliance Center will not appear to users in Outlook on the web and Outlook 2013 and later until you turn off the tips in the Exchange admin center.

This ensures that your current Exchange mail flow rules will continue to work until you choose to switch over to the Security & Compliance Center.

Note that while policy tips can draw only from a single location, email notifications are always sent, even if you're using DLP policies in both the Security & Compliance Center and the Exchange admin center.