Filename: microsoft-ms101-9-6-1-manage-dlp-policy-matches
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Configure Data Loss Prevention (DLP)
EpisodeName: Manage DLP Policy Matches
Description: Adam and Wes discuss the steps necessary to help you successfully manage DLP policy matches.

Manage DLP Policy Matches

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

==========

Manage DLP Policy Matches

How do I customize built-in sensitive information types?

```
• Customize built-in sensitive information types: altering the XML information
that defines how rules detect information. You use PowerShell to export the
sensitive information types to XML.

• Create your own Sensitive Information types: Use the wizard in
o365 Security & Compliance
```

What about creating a custom dictionary?

A keyword dictionary can hold up to 100,000 words & you can have multiple dictionaries.

Steps:

```
1. Create a text file with all words needed; one word per line. Needs to be
encoded using UNICODE. Save locally & note path for use in step 3 below.

2. Open PowerShell & connect to the o365 Security & Compliance Center

3. Navigate to the path where you saved file in Step 1 inside PowerShell, then
type the following:

$File = Get-Content .\DLP-<name of file from Step 1 above>.txt -Encoding Byte -ReadCount 0

4. Run the following command from PowerShell:

New-DLPKeyWordDictionary -Name <name of dictionary> -Description '<description>' -FileData $File
```

What is a Document Fingerprint and how do I create one?

Document Fingerprinting is a Data Loss Prevention (DLP) feature that converts a standard form into a sensitive information type, which you can use to define transport rules and DLP policies.

For example, you can create a document fingerprint based on a blank patent template and then create a DLP policy that detects and blocks all outgoing patent templates with sensitive content filled in.

Optionally, you can set up Policy Tips to notify senders that they might be sending sensitive information, and the sender should verify that the recipients are qualified to receive the patents.

NOTE: This process works with any text-based forms used in your organization.

What file types are supported?
https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/inspect-message-attachments?redirectedfrom=MSDN

NOTE: Neither transport rules nor Document Fingerprinting supports the .dotx file type, which can be confusing because that's a template file in Word. When you see the word "template" it refers to a document that you have established as a standard form, not the template file type.

Limitations of document fingerprinting:

The Document Fingerprinting DLP agent will not detect sensitive information in the following cases:

```
• Password protected files
• Files that contain only images
• Documents that do not contain all the text from the original form used to
create the document fingerprint
```

CAN ONLY BE CREATED USING PowerShell !!!