Manage Sensitive Info Types

At the end of this episode, I will be able to:

1. Implement and manage sensitive info types by using keywords, keyword lists, or regular expressions

Learner Objective: *Manage sensitive info types*

Description: In this episode, you will learn about the pre-created sensitive info types in Microsoft Purview. You will also learn how easy it is to create your own sensitive info types for use in governance and compliance.

- Purview is equipped with search and recognition patterns for sensitive information types, such as credit cards numbers and addresses.
- These sensitive information types are defined by patterns using regular expressions, or functions, or keywords, or checksums.
- There are over 100 built-in sensitive information types.
- You can create your own sensitive information types in order to identify your own organization-specific information types. For example, perhaps employee IDs or project numbers or names would be key criteria specific to your organization.
- The components of the sensitive information types include:
    - Primary pattern
    - Additional evidence
    - Character proximity
    - Confidence level
- Special features of custom sensitive information types include:
    - Exact Data Match (EDM) based classification
    - Document Fingerprinting
    - Keyword dictionaries
- To create your own sensitive information type - in the Compliance Center, go to Data classification > Classifiers > Sensitive info types and choose Create sensitive info type.

Additional Resources:

Create and Manage Sensitive Information Types
https://learn.microsoft.com/en-us/training/modules/create-manage-sensitive-information-types/