Protecting Your Data with Microsoft Purview Information Protection

David Drever

david.drever@protiviti.com

https://prairiedeveloper.com

Microsoft 365 CONFERENCE

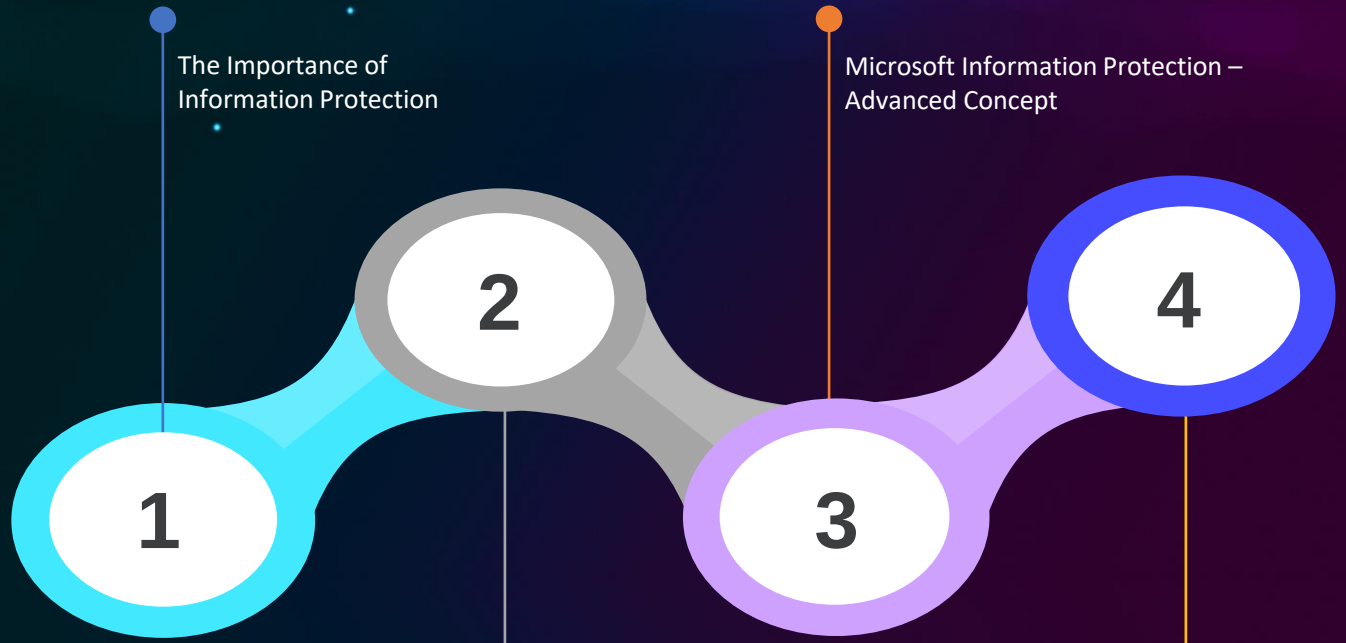
Microsoft Viva
Microsoft Teams
Microsoft SharePoint
Microsoft Power Platform

CO PRODUCED BY MICROSOFT AND M365 CONFERENCE

2022 LAS VEGAS

Let’s Connect

Agenda



1. The Importance of Information Protection
2. Microsoft Information Protection
3. Microsoft Information Protection – Advanced Concept
4. Deploying Microsoft Information Protection

Importance of Security In the Cloud

Businesses are moving to the cloud

- 73% of enterprises have at least one component of their business in the cloud
- Some enterprises predict they will invest $3.5 million in cloud technology (Apps, services, etc)
- Many businesses store PII data digitally, including within cloud technologies
- Less than half of organizations in the cloud have a formal cloud security policy

Security Breaches… they happen

- Estimation of 79% of large U.S. businesses and 49% of large Canadian businesses experienced a data breach in 2021
- Estimation of 61% of SMB U.S. businesses and 50% of SMB Canadian businesses experienced a data breach in 2021

Microsoft Information Protection

Principals of Information Protection

Identify

- Microsoft Information Protection provides organizations with the ability to locate and identify sensitive information within their infrastructure. It can find information based on established or custom categories developed by the business.

Classify

- Once identified, information can be classified based on the organization's sensitivity classification policy. The information allows users to understand the sensitivity of the information they are working with.

Protect

- Once classified, necessary protections can be applied; this can range from automatically adding headers, footers, or watermarks to full encryption of the content.

Sensitivity Label Overview

To plan and prepare for the implementation of MIP labels, it is best to understand the capabilities and plan accordingly.

Sensitivity Label Capabilities:

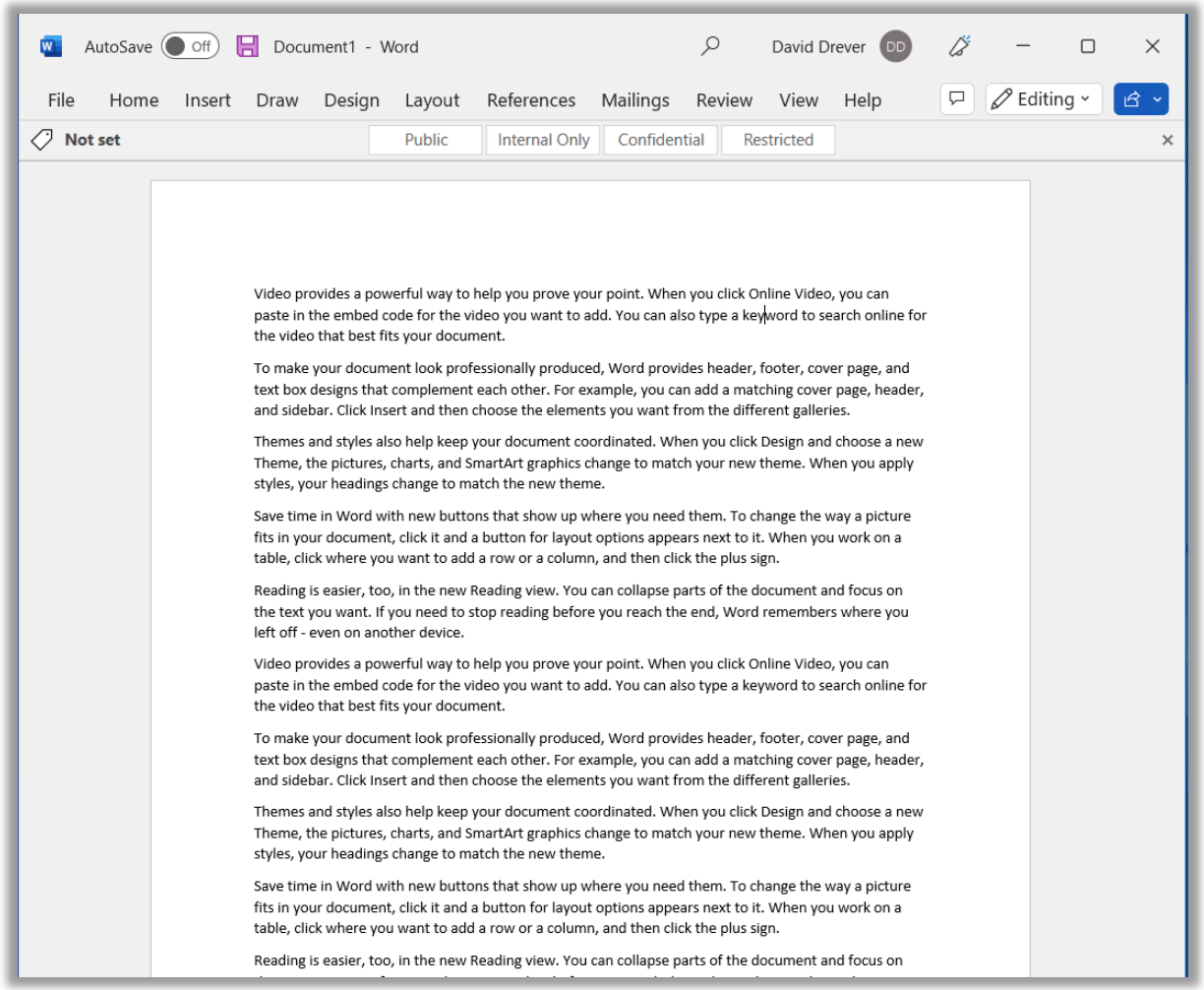
- Content Markup when labels are applied to content:
  - Headers and/or Footers
    - Multiple colors available
    - Left, Center, or Right justified
    - Variable font size
  - Watermark
    - Multiple colors available
    - Variable font size
    - Variable font direction

Sensitivity Label Overview

To plan and prepare for the implementation of MIP labels, it is best to understand the capabilities and plan accordingly.

Sensitivity Label Capabilities:

- Content Markup when labels are applied to content:
  - Headers and/or Footers
    - Multiple colors available
    - Left, Center, or Right justified
    - Variable font size
  - Watermark
    - Multiple colors available
    - Variable font size
    - Variable font direction

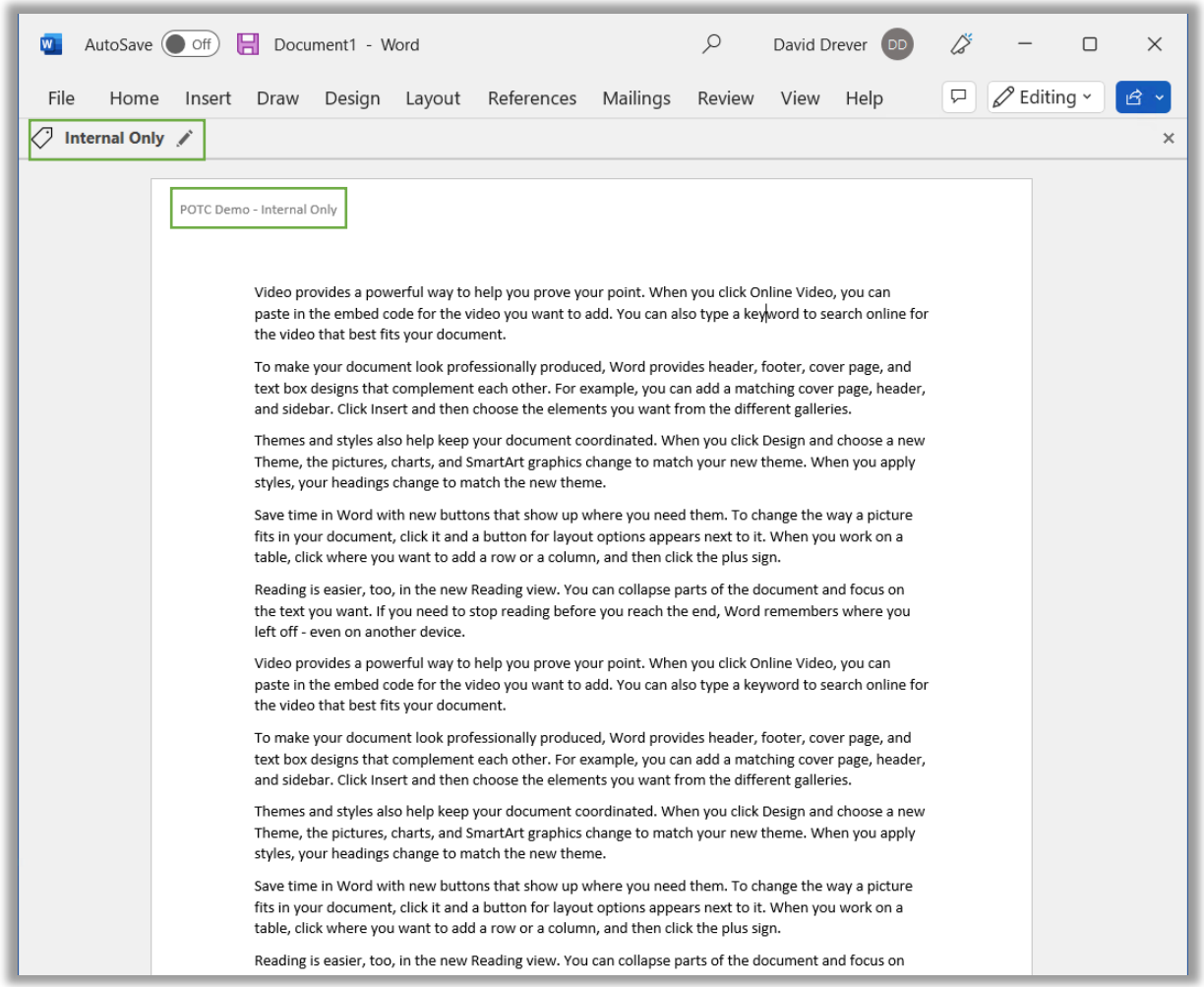


Sensitivity Label Overview

To plan and prepare for the implementation of MIP labels, it is best to understand the capabilities and plan accordingly.

Sensitivity Label Capabilities:

- Content Markup when labels are applied to content:
  - Headers and/or Footers
    - Multiple colors available
    - Left, Center, or Right justified
    - Variable font size
  - Watermark
    - Multiple colors available
    - Variable font size
    - Variable font direction

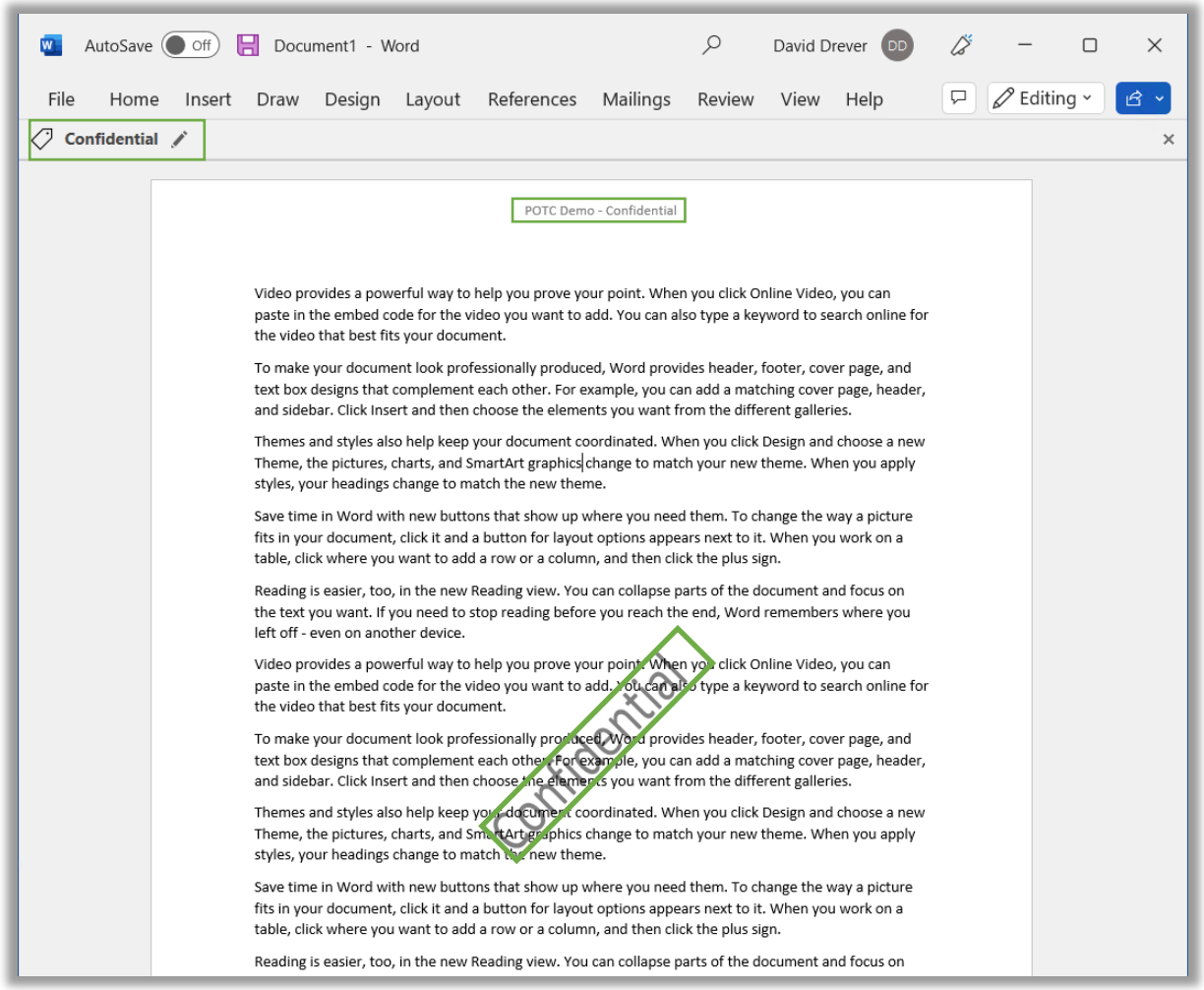


Sensitivity Label Overview

To plan and prepare for the implementation of MIP labels, it is best to understand the capabilities and plan accordingly.

Sensitivity Label Capabilities:

- Content Markup when labels are applied to content:
  - Headers and/or Footers
    - Multiple colors available
    - Left, Center, or Right justified
    - Variable font size
  - Watermark
    - Multiple colors available
    - Variable font size
    - Variable font direction



Sensitivity Label Overview

To plan and prepare for the implementation of MIP labels, it is best to understand the capabilities and plan accordingly.

Sensitivity Label Capabilities:

- Content Markup when labels are applied to content:
  - Headers and/or Footers
    - Multiple colors available
    - Left, Center, or Right justified
    - Variable font size
  - Watermark
    - Multiple colors available
    - Variable font size
    - Variable font direction
- Encryption
  - Independent of location security. Dependent on the label configurations
  - Two encryption options:
    - Administrator Defined Permissions
      - Control when access to content expires (default is never)
      - Allow or Reject Offline Access
    - User Defined Permissions
      - User can assign permissions when the label is applied
  - Double-Key Encryption
    - Second encryption appliance run by the organization that encrypts on top of MIP Encryption

Microsoft Information Protection Advanced Concepts

Site and Group Sensitivity Labels

Applies Information Protection Controls to Sites and Groups

- Does NOT apply default sensitivity to content within the site.
- Applies additional controls to sites:
  - Block external users
  - Enforce managed devices
  - Site Owner permission granting controls
- Apply Authentication Contexts to sites for use with Conditional Access
- Automatically notifies users and administrators if highly sensitive content is uploaded to the site.

Automating Sensitivity Labels

Why should we consider this? Users will take care of it, right?

- Complex classification systems make determining the proper sensitivity label difficult
- Users will forget if not forced to by a sensitivity policy
- User's feel they don't have time to "deal" with sensitivity labels
- Sometimes only the default (easiest) solution is selected when a more sensitive solution is required
- Users lack sufficient training to support the organization's sensitivity classification requirements.

Automating Sensitivity Labels

Auto-Apply Settings on Sensitivity Label

- Via MIP client (built-in to Microsoft Office or add-on) scans content constantly for changes that fall under any rules applied to the environment through the sensitivity label configuration
- If sensitive information is found two options can occur:
  - Sensitivity label is enforced
  - Sensitivity label is recommended

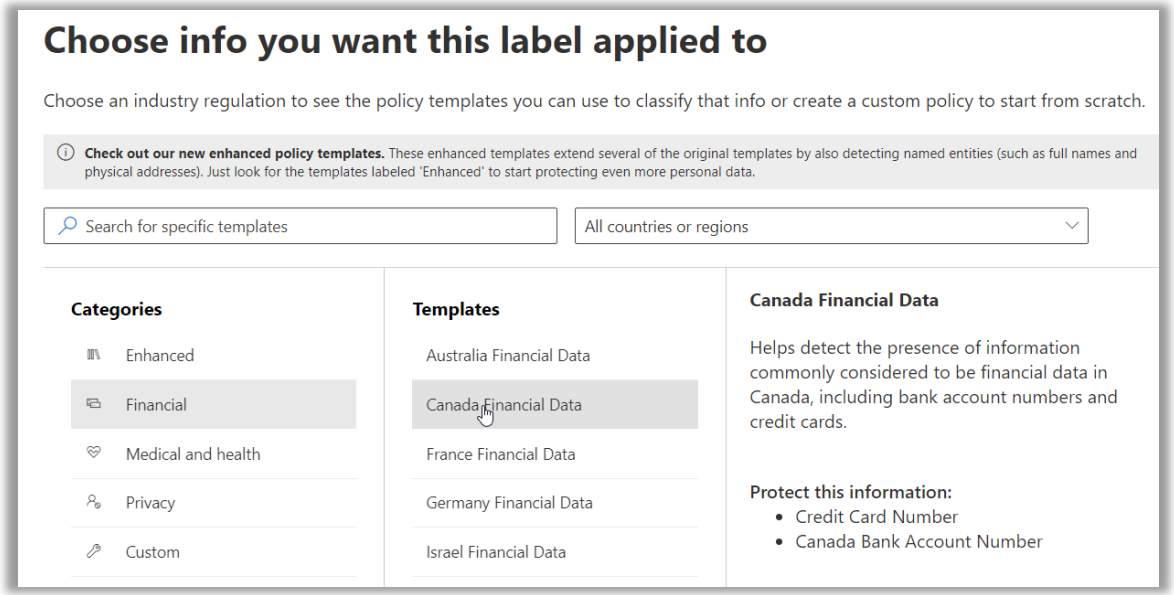
Auto-Apply Sensitivity Label Policy

- Applies sensitivity labels to content at rest in SharePoint Online (Teams), OneDrive, and Exchange
- Can apply to on-premises content as well via AIP Scanner
- PDF and Office app scanning supported in Exchange

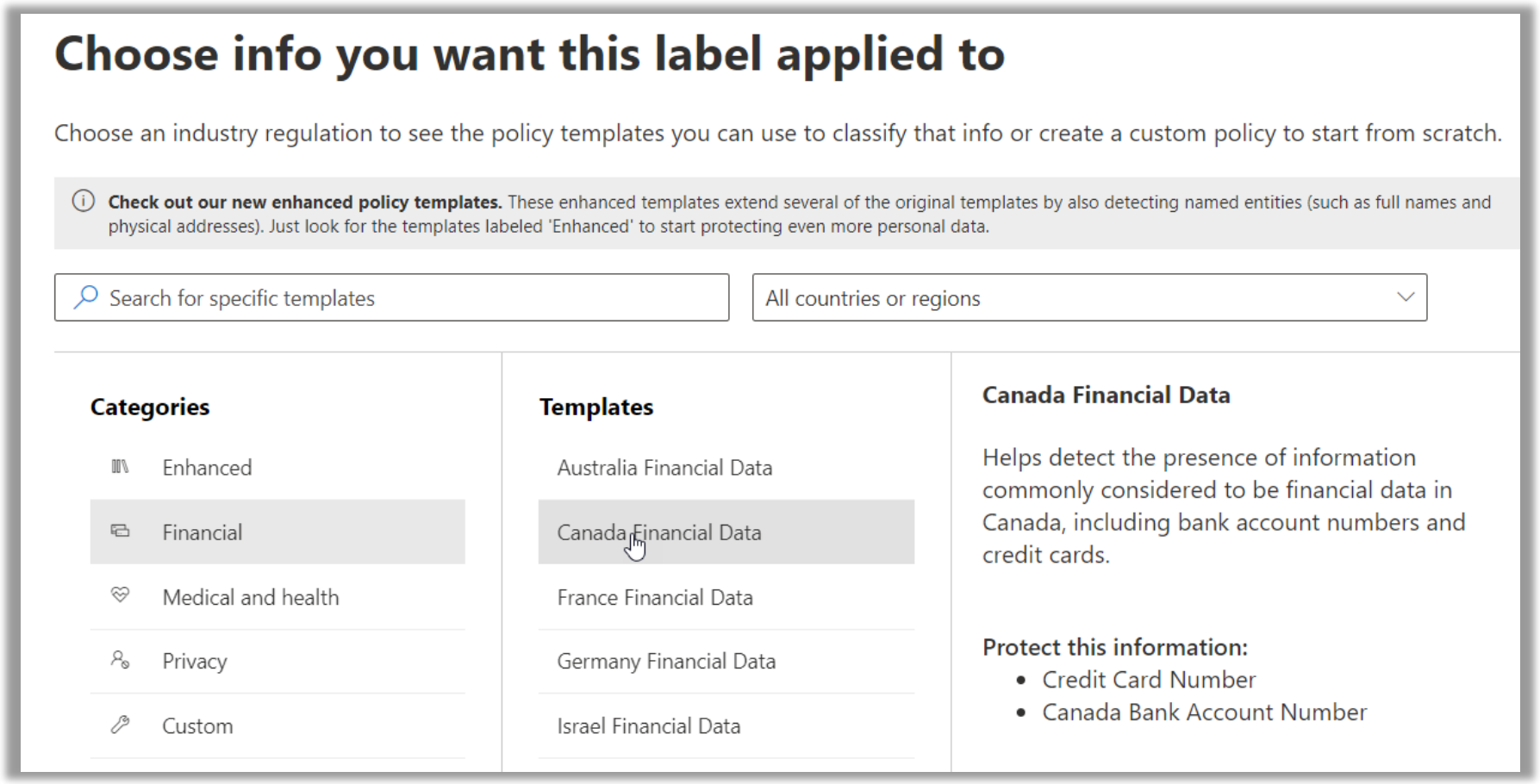
Automating Sensitivity Labels – Methods to Apply

Sensitivity Type

- Auto Application Availability:
  - Label Auto-Apply Configurations
  - Auto-Apply Label Policies
- Locations:
  - Exchange
  - SharePoint
  - OneDrive
- Select from 300 existing sensitive information type templates or create custom sensitivity types
- Customize based on the instance count
  - Number of times the sensitive instance type exists in document before rule fires



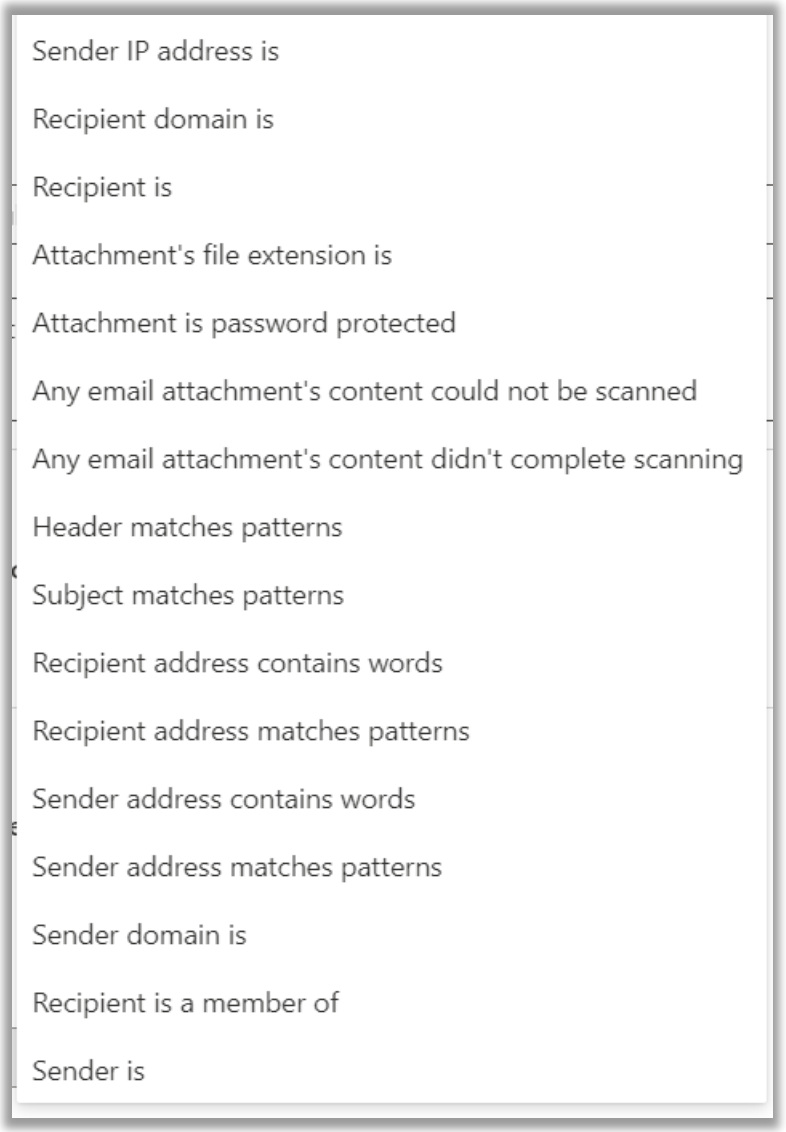
Automating Sensitivity Labels – Methods to Apply



Automating Sensitivity Labels – Methods to Apply

Email Properties

- Available for:
  - Auto-Apply Label Policies
- Locations:
  - Exchange only



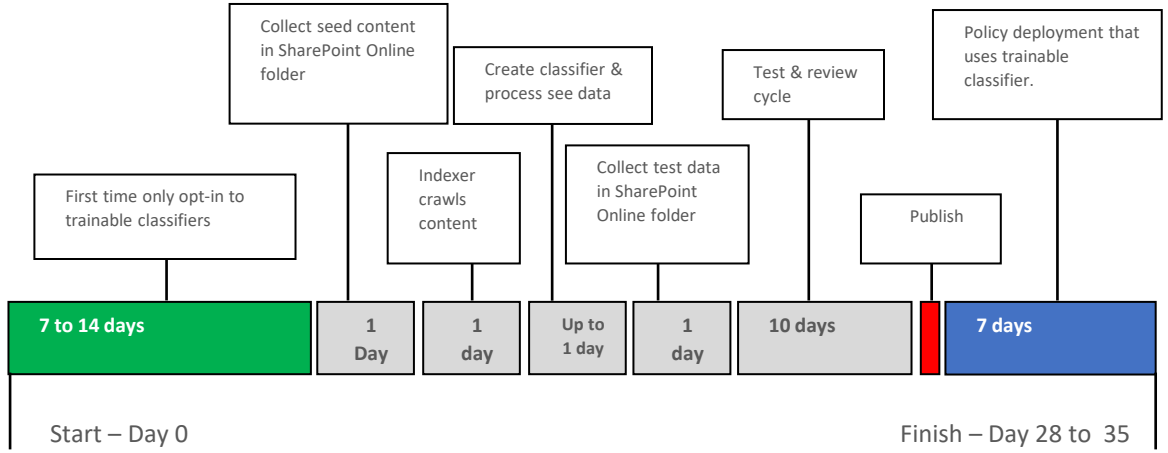
Automating Sensitivity Labels – Methods to Apply

Trainable Classifier

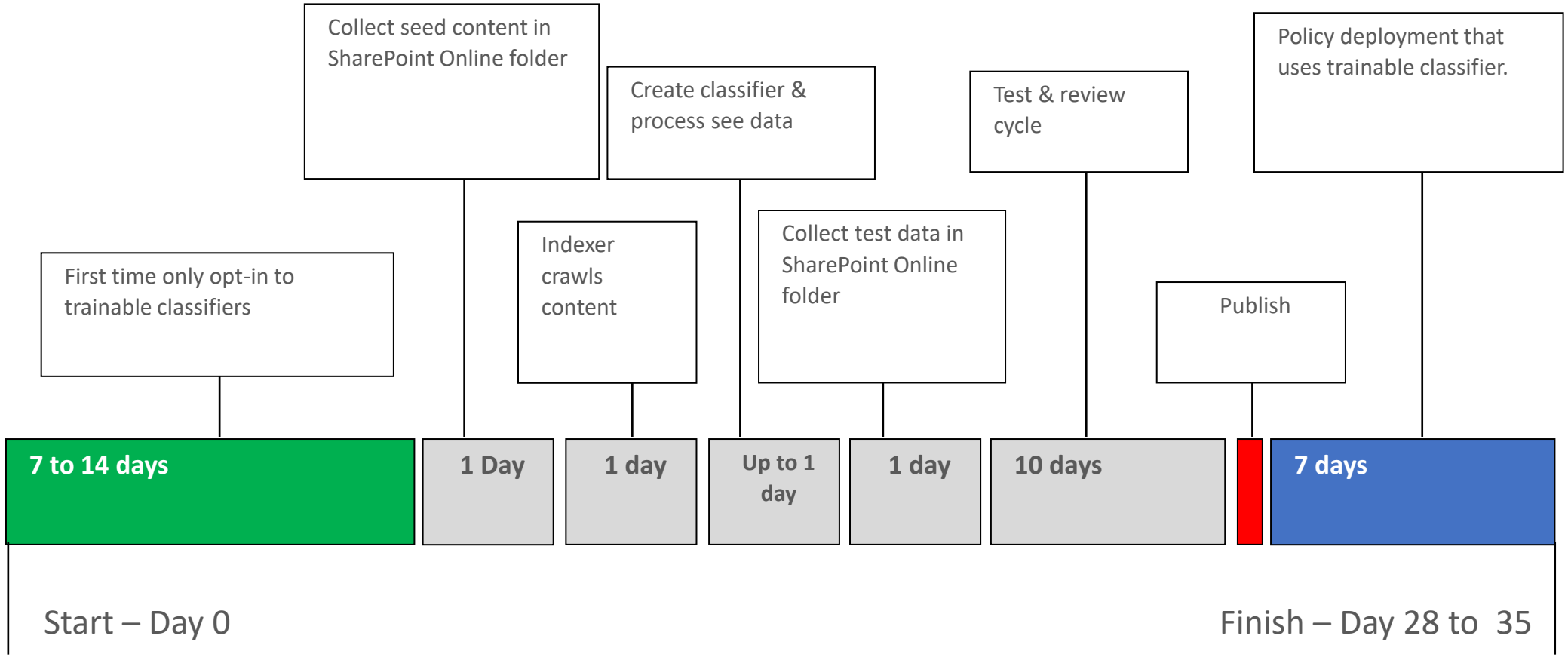
- Machine Learning/AI
  - Capable of recognizing types of content
  - Instruct system on the types of documents within the organization

- Available for:
  - Label Auto-Apply Configurations

- Organizations can create their own trainable classifiers



Automating Sensitivity Labels – Methods to Apply



Deploying Microsoft Information Protection

Controlled Implementation

A key consideration of the strategy is the implementation approach. To avoid pitfalls often encountered in rapid rollouts, it is recommended a phased approach known as Crawl, Walk, and Run

- **Crawl**
  - Define Sensitivity within the organization.
  - Immediate changes that focus on being non-intrusive to end-users.
  - Prepares organization for future phases

- **Walk**
  - Intermediate, but still near-time changes that allow for further control of processes.
  - More user-impacting than Crawl

- **Run**
  - Long-term changes that require more planning and preparation, such as automation of tasks or implementation of strategic goals.
  - Complex processes

Tools Required for MIP

Microsoft Information Protection stand-alone client is required to support files that are not natively supported within MS Office

- Stand-alone tool for encrypting all file types within Windows, MacOS, iOS, and Android operating systems
- Provides ability to encrypt content for systems lacking necessary Office build and files not supported by the native client within MS Office

MIP Add-On for Acrobat Reader

- Allows Acrobat Reader to decrypt content encrypted by Microsoft Information Protection
- Built-in to Adobe Acrobat since June 2022

What to consider before deployment

While planning a phased implementation is important, there are some activities that must first be considered and planned before implementation begins.

Organizational Change Management

- Needs to start at Day 1 of the project
- Users need to understand:
  - Why this is being implemented
  - How it will affect them
  - What is expected of them
  - The benefit to them and the organization
- Training for end-users should be designed and training sessions planned
- Planning and design of notifications and alerts

What to consider before deployment

While planning a phased implementation is important, there are some activities that must first be considered and planned before implementation begins.

Governance

- Creation or review of sensitivity classification policies (non-technical)
- Information protection and the tools and processes supporting it are dynamic and change often. Additionally, changes or exceptions may be required. A committee should be created with the authority to review changes, requests, suggestions, etc. and provide direction and decisions on them.
- Committee should be made up of IT, Security\Privacy, and business representatives
- Create and ratify a framework from which information protection is based upon.

What to consider before deployment

While planning a phased implementation is important, there are some activities that must first be considered and planned before implementation begins.

Super User Role

- Highly specialized role to decrypt all data that has been encrypted within the M365 tenant.
  - Limited to files the user has access to
- If possible deploy using Privileged Access Groups (PAG) with full approval enabled.
- If PIM not yet enabled, deploy to as few users as possible

Crawl Phase

The crawl phase focuses on the pilot and initial rollout of MIP labels and label policies to small, but meaningful “pilot group” within the organization. Notifications and training should begin

MIP Label Use Preparation and Distribution

- Ensure all workstations and devices meet the minimum office build required to support the options desired with MIP
  - Install the MIP client to all desktops lacking the required office build
  - Consider installing to all devices to support not natively-supported filetypes
  - Deploy Adobe Acrobat MIP Add-On to all workstations that do not have the required June 2022 or later build

- Manually applied labels only should be deployed to the pilot group.
- Allow time for the pilot group to test the usage of the labels.
  - Review results and update implementation plan as required
- Begin to deploy to remaining users as they receive the necessary training
- Deploy Site and Group sensitivity labels to identified administrators

Walk Phase

The walk phase should not begin until all users have been implemented under the crawl phase. In this phase more advanced processes and features are introduced to the organization.

Automation of Sensitivity Labels

- Begin deployment of automation controls within the MIP labels.
  - Focus on OOTB sensitivity types
- Create auto-apply label policies to update content stored within Microsoft 365 storage locations
  - Ensure simulation is enabled first before fully activating
- Design and implement a charter for the governance committee to follow
- Identifying content to be used for trainable classifiers (feeds into Run Phase)

Run Phase

The run phase is considered the final stage of an implementation project. In this stage the more complex automation processes are focused on. All Walk Phase components should be implemented before moving to Run.

Complex Configurations

- Begin building trainable classifiers within Purview
- Implement and monitor sensitivity based on the classifiers
- If User Defined Permission labels have been deployed, enable co-authoring of encrypted labels within the tenant
- If auto-apply configurations created in the walk phase meet the needs of the organization, consider enforcing the application of sensitivity labels as opposed to recommending they be applied.
- If required, use Authentication Context to integrate sensitivity as a signal to Conditional Access within the environment

Face the Future with Confidence

protiviti®