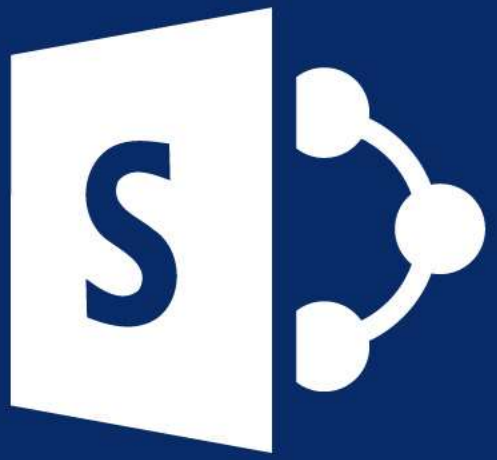


4 Easy Steps to SharePoint Data Compliance

Modern data protection made simple

colligo

by @JoelOleson

MVP Office Apps & Services

4 Steps to SharePoint Data Compliance

colligo

Presenters

Joel Oleson

SharePoint MVP

- Microsoft Regional Director
- 19-year SharePoint Veteran
- 7 years at Microsoft
- First SharePoint IT Admin

Roland Reddekop

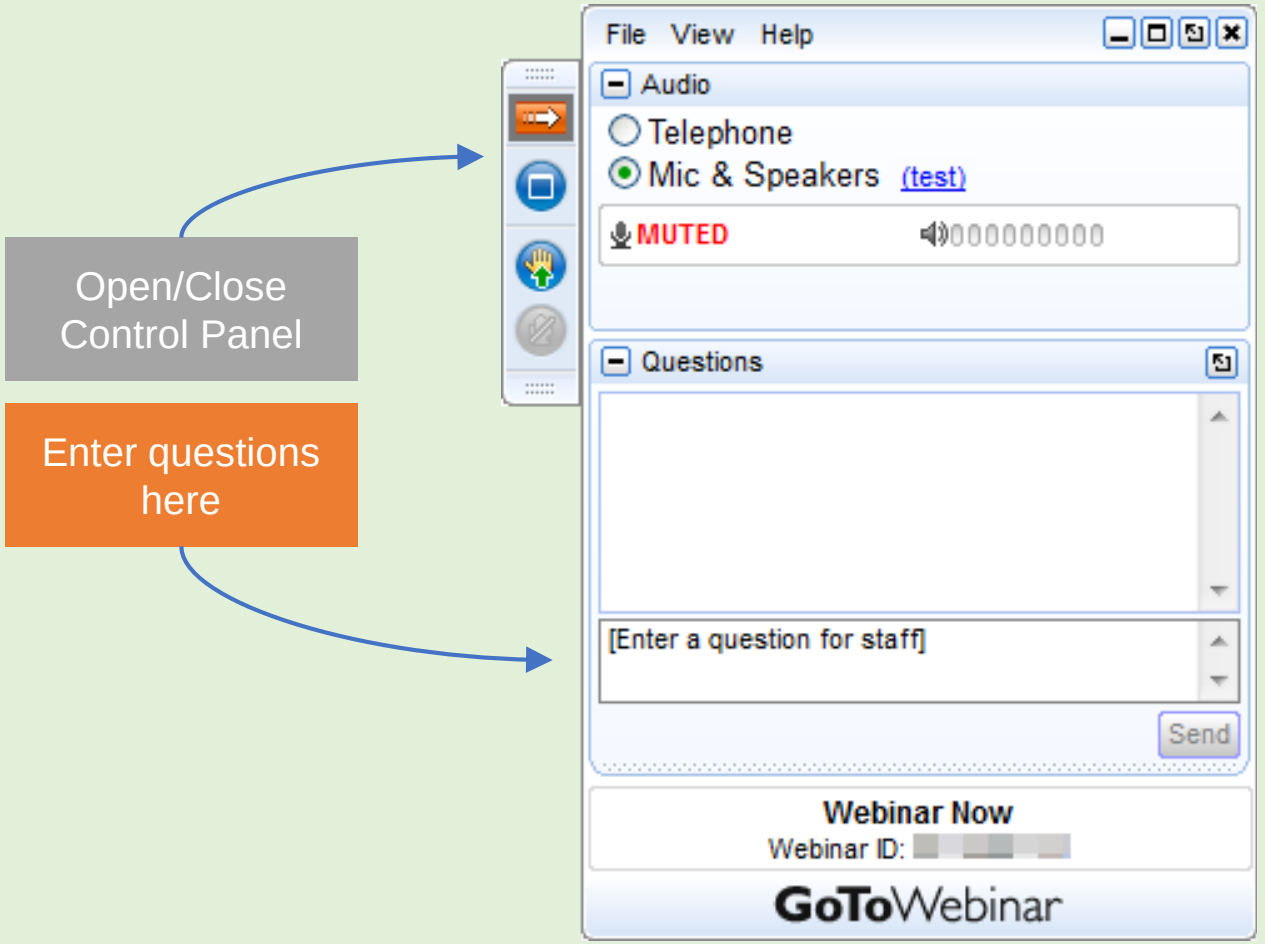
Presale Engineer, Colligo

- Microsoft Partner – Gold Application Development


hp

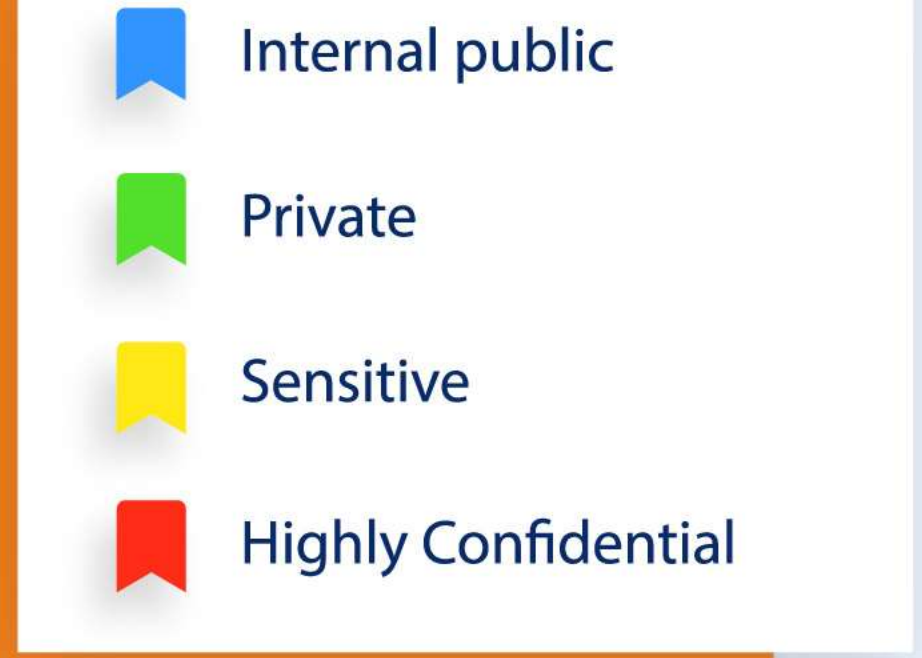
Logistics

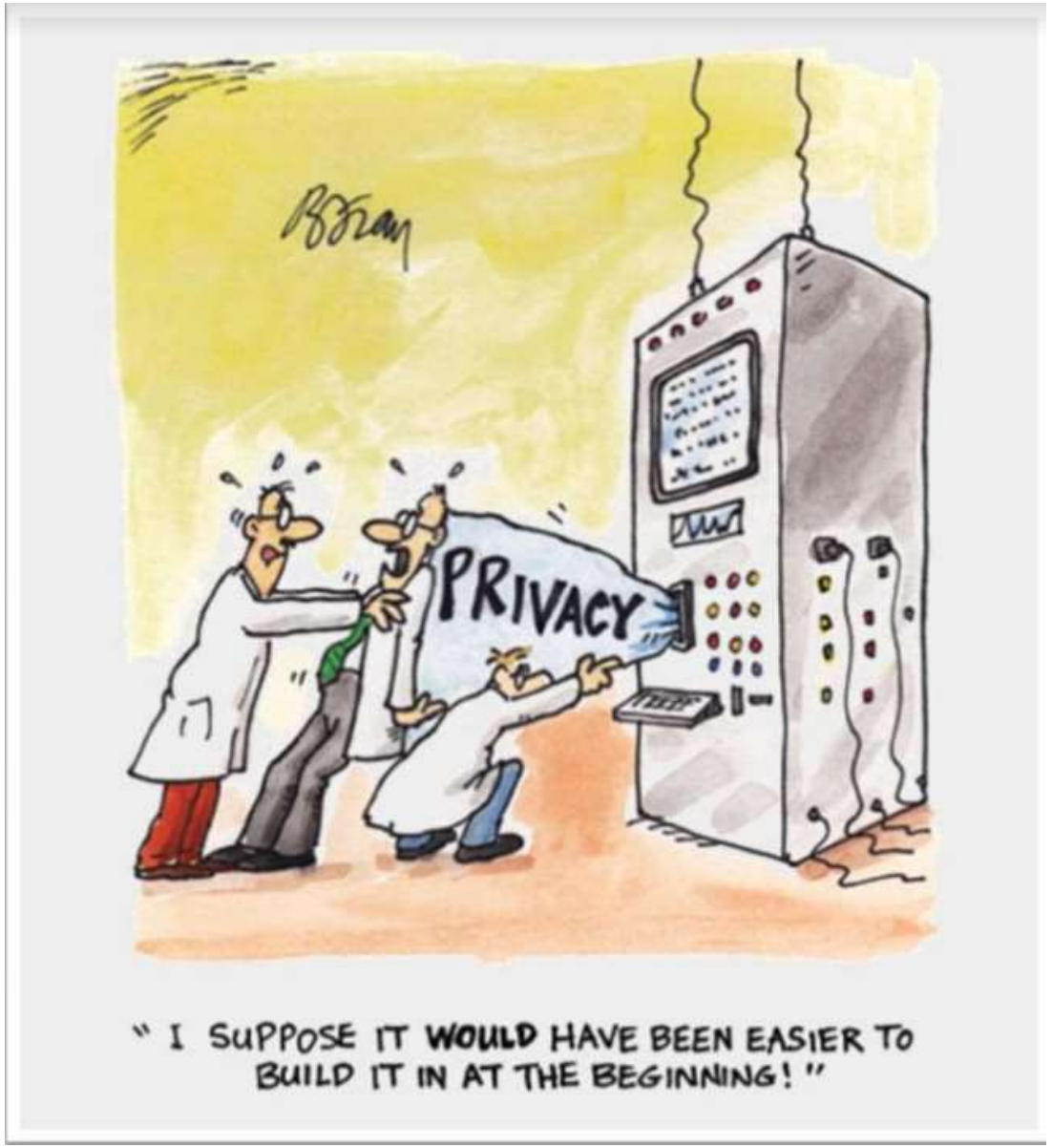
- Webinar will be 60 minutes
- You will receive a recording of the webinar by email
- Enter questions in the Control Panel



Step 1

Determine Label Names




PRIVACY
" I SUPPOSE IT WOULD HAVE BEEN EASIER TO BUILD IT IN AT THE BEGINNING! "

Office 365 Classification Labels

Samples

SharePoint Site Level		Sensitivity Label name	Govt sample
Baseline	Public	No Label	Declassified
Baseline	Private	Internal Only	Classified
Sensitive Protection		Confidential	Secret
Highly Confidential		Highly Confidential	Top Secret

Team Site Classification

Highly Classified

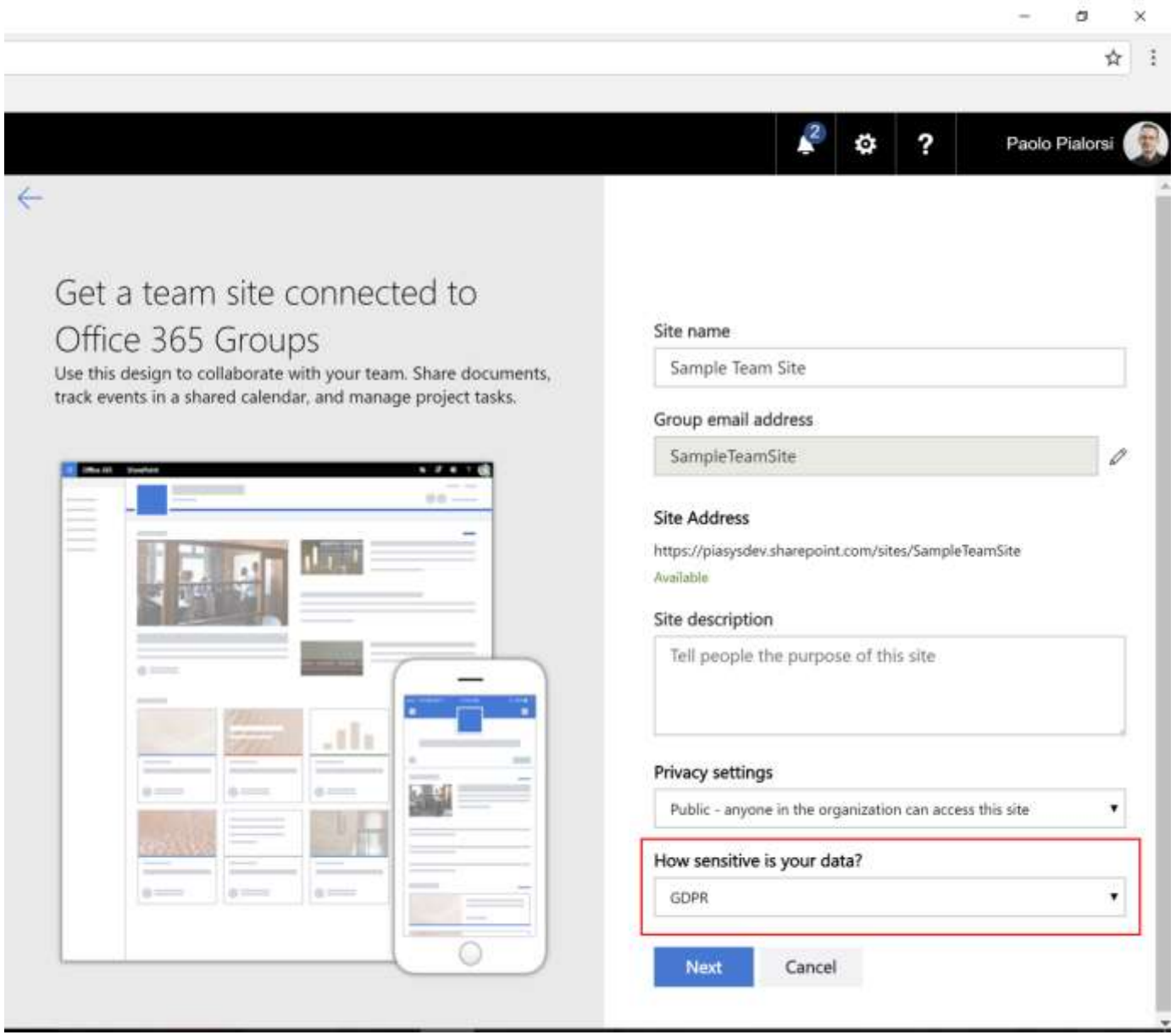
Classified
(Internal Only)

Internal Public
Social Groups &
Comm Sites

Partner
Vendor Extranet

Regular Security Review and Audit

Site Information Panel: Privacy & Site Classification



File Plan: Sample Retention

SUMMARY OF RETENTION PERIODS UNDER US FEDERAL LAWS:

Document Description	Number of Years
Employee Data and Personnel Files	3 years.
Payroll and Wage Data	3 years.
Family, Medical, and Parental Leave	3 years.
Collective Bargaining/Union	3 years.
Employee Benefit Plans	6 years.
Background Checks	5 years.
Hazardous Material Exposure	Duration of employment + 30 years.
Injury and Illness Incident Reports	5 years.
Employee Tax Records	4 years.
Form I-9 Employment Eligibility Verification	Duration of the employee's employment with the employer, plus the longer of 3 years from date of hire or 1 year from date of termination.
Labor Condition Application (LCA) Public Access File (PAF)	Longer of 1 year from LCA expiration or 1 year from the last date anyone is employed under LCA.
Permanent Labor Certification Audit File	5 years from the PERM filing.

Sample Policy or Regulation

Requirements Under HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule establishes federal standards to protect individuals' medical records and other personal health information. The HIPAA Privacy Rule does not include medical record retention requirements. These requirements are governed by state rules regulating how long medical records should be retained. Instead, HIPAA requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other protected health information (PHI) for whatever period such information is maintained by a covered entity, including through disposal. See 45 C.F.R. § 164.530(c). HIPAA allows documents to be maintained in electronic form. See 45 C.F.R. § 164.316(b)(1).

Additionally, the following documents should be retained:

- The policies and procedures for complying with the HIPAA Privacy Rule;
- Any communication required by the HIPAA Privacy Rule to be in writing; and
- Any action, activity, or designation required to be documented by the HIPAA Privacy Rule.

Generally, companies should retain the above-described documentation for six years from the date of its creation or the date when it was last in effect, whichever is later. See 45 C.F.R. § 164.316(b)(2)(i).

DEMO: Information Protection in Office 365

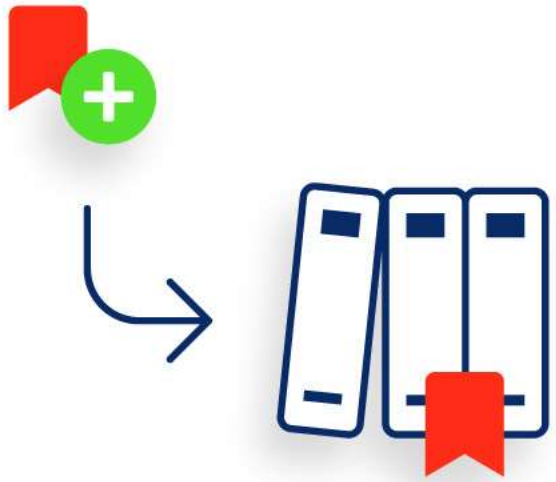
https://protection.office.com

https://compliance.office.com

Why Use Labels?

colligo

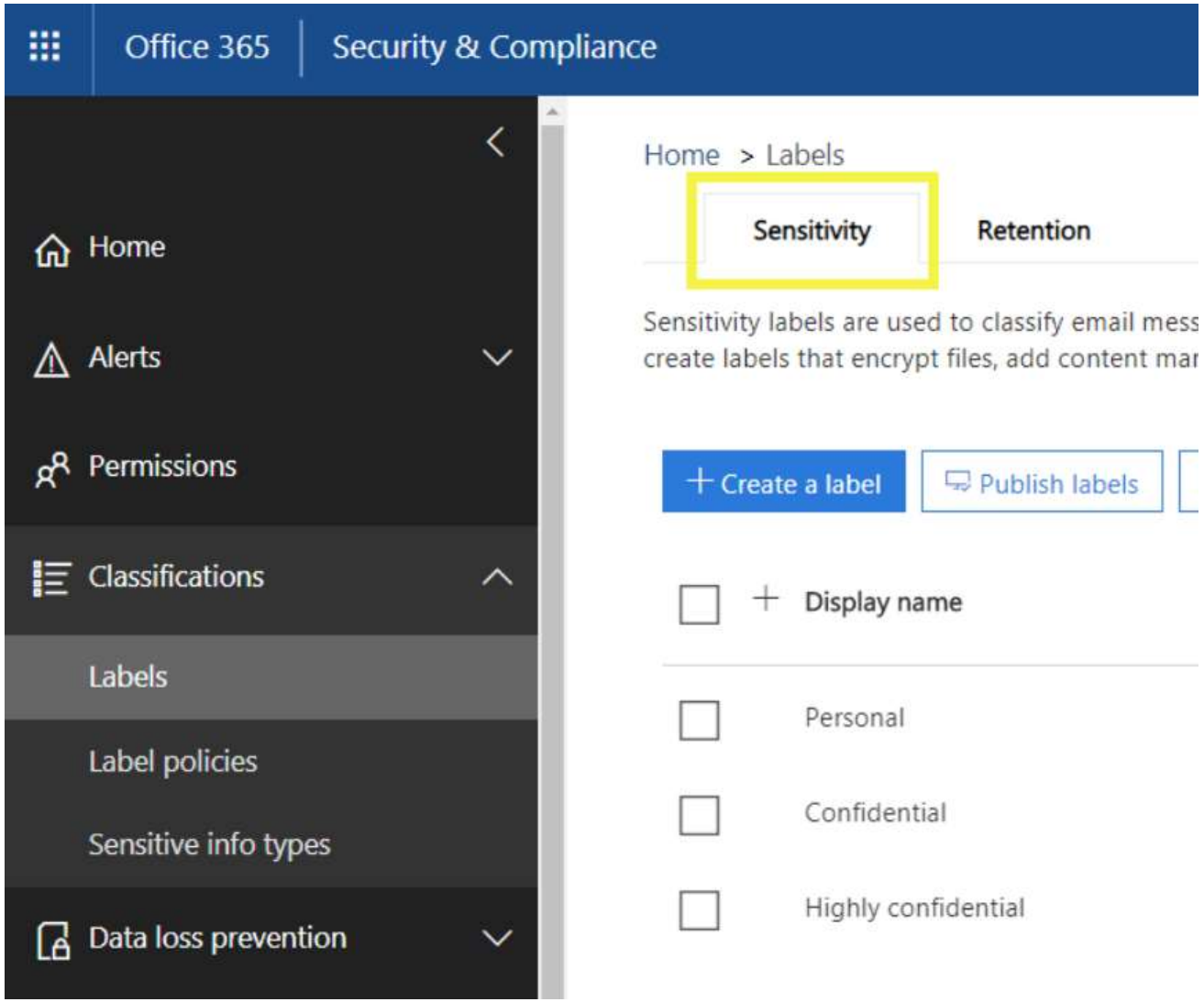
Enforce encryption or watermarks.	Prevent sensitive Content from Leaking	Classification of Content	Dispose or Retain & Review
• Labels can be used to encrypt content and apply a watermark.	• Endpoint protection can warn or block content from being copied to Twitter or Gmail or USB drive	• Focus on content that matters most. Generate usage reports, enforce policies	• Retention policies can kick off workflows to enforce retention policies

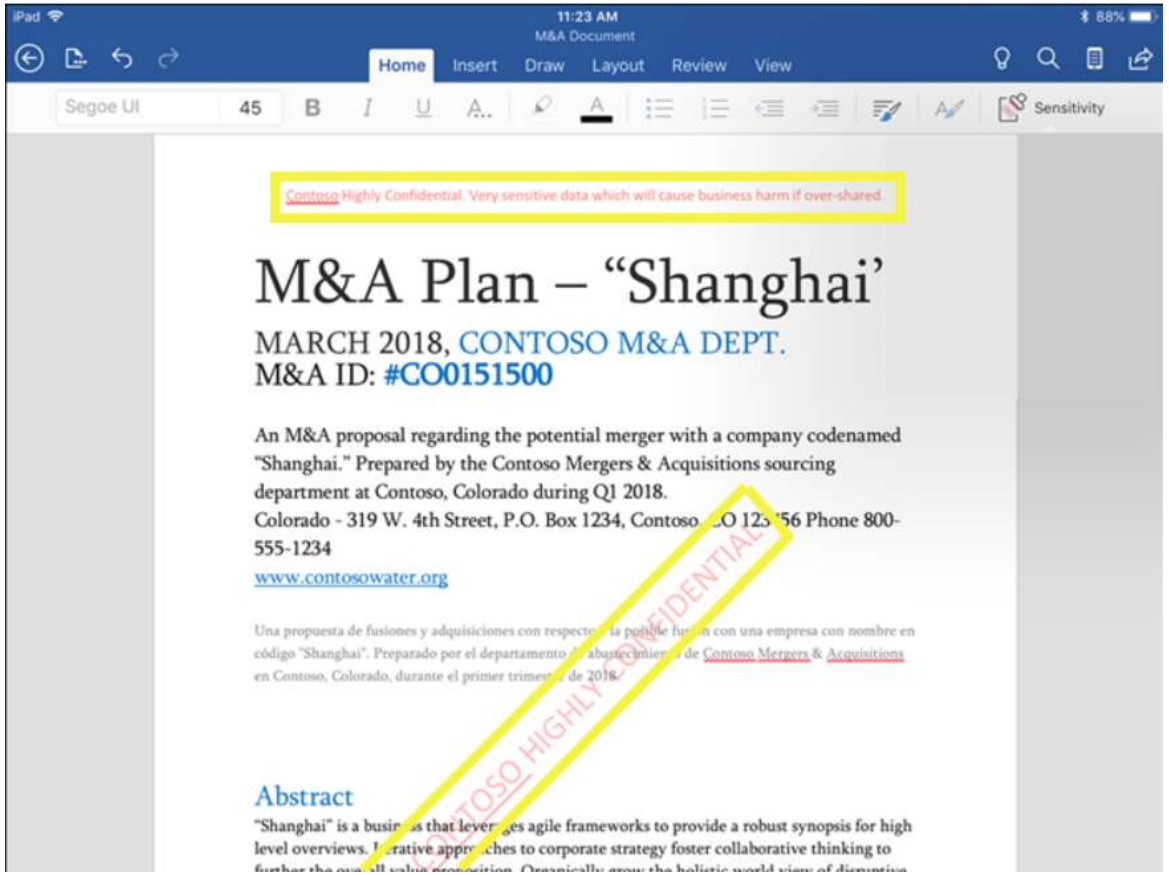


Create, Publish and Apply Labels to Libraries

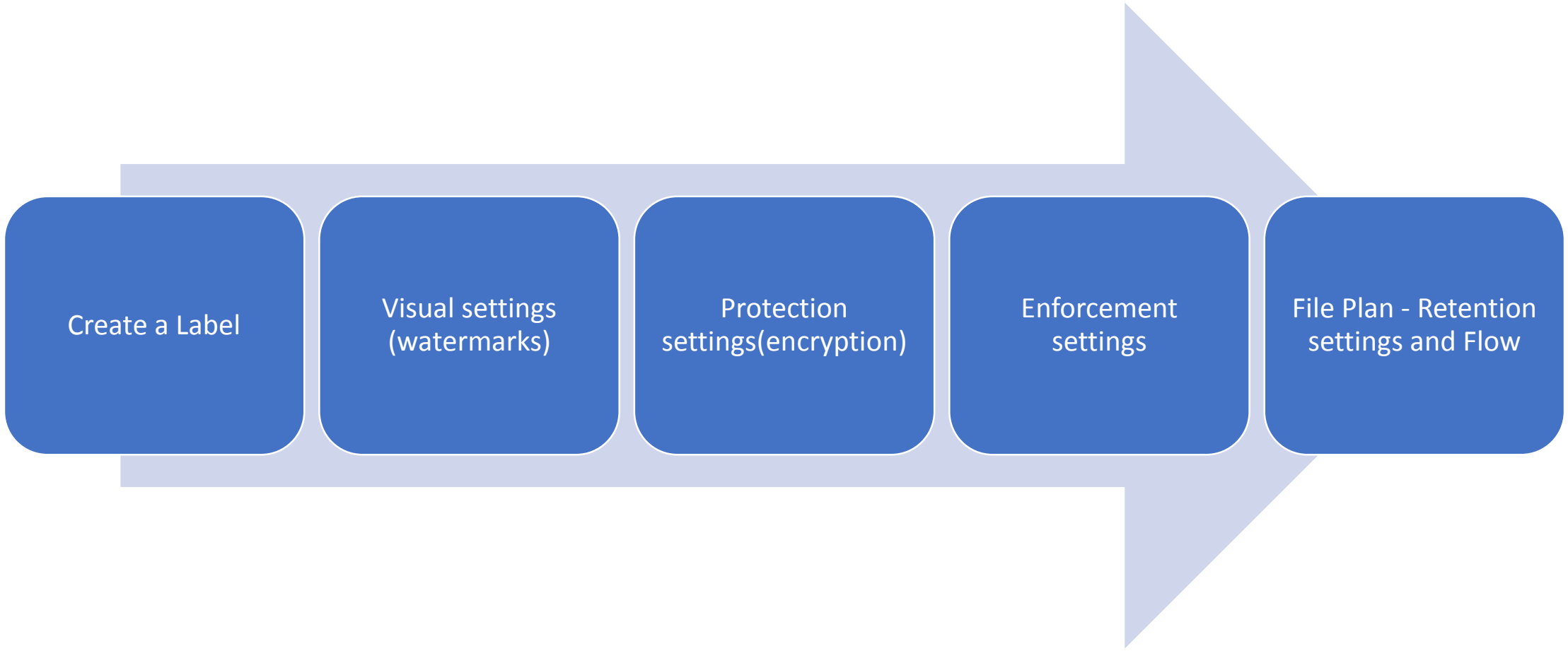
Step 2

Create & Publish Labels





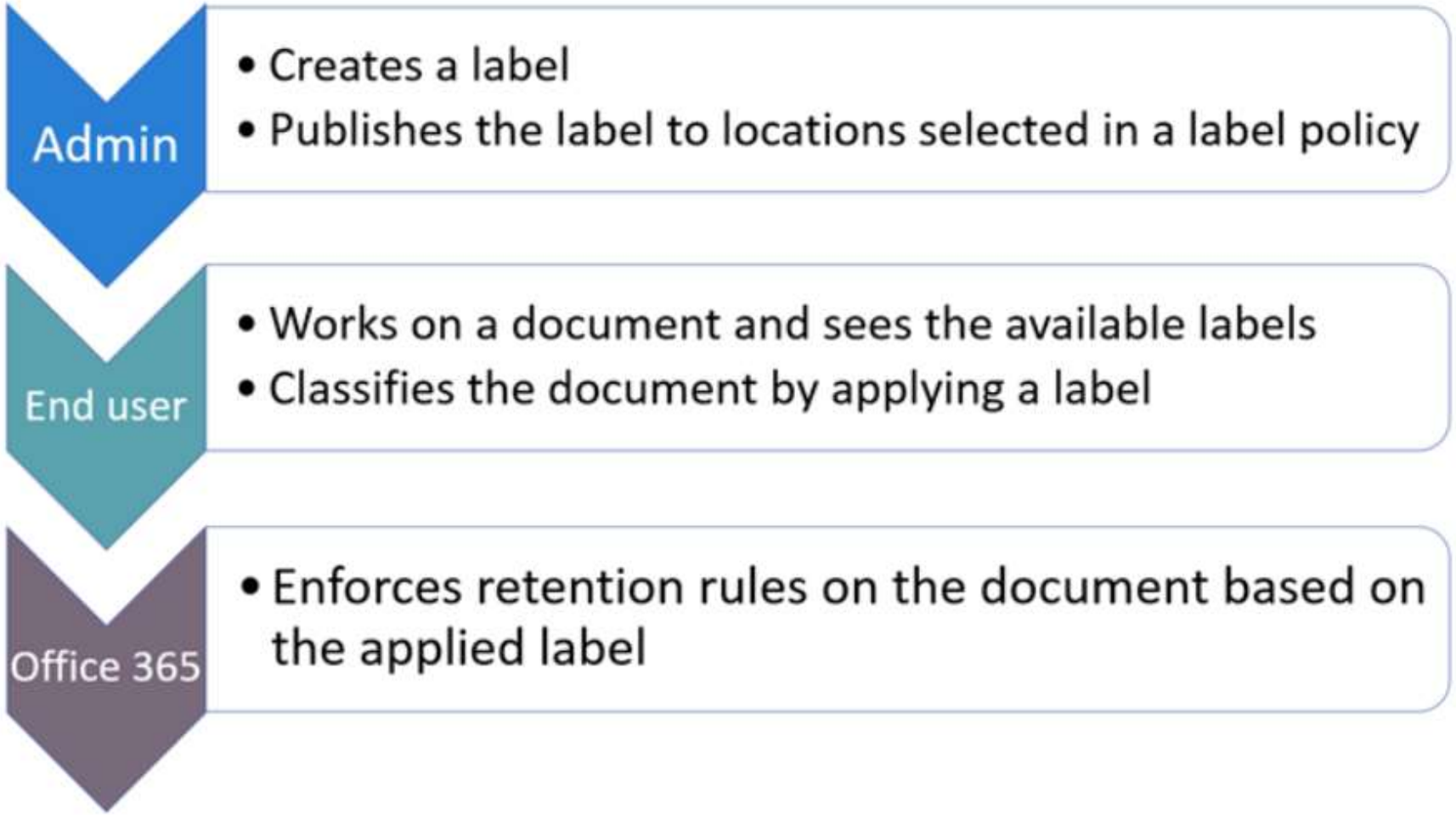
Unified labelling is coming together



Practical Guidance

- Create the desired labels and publish. It can take up to 12 hours for publish to complete.
- For the desired SharePoint sites, edit the document library settings to apply a label to items in the library.
- Create DLP policies to take action on 80 sensitivity based on the labels.

How Retention Labels Work with Label Policies



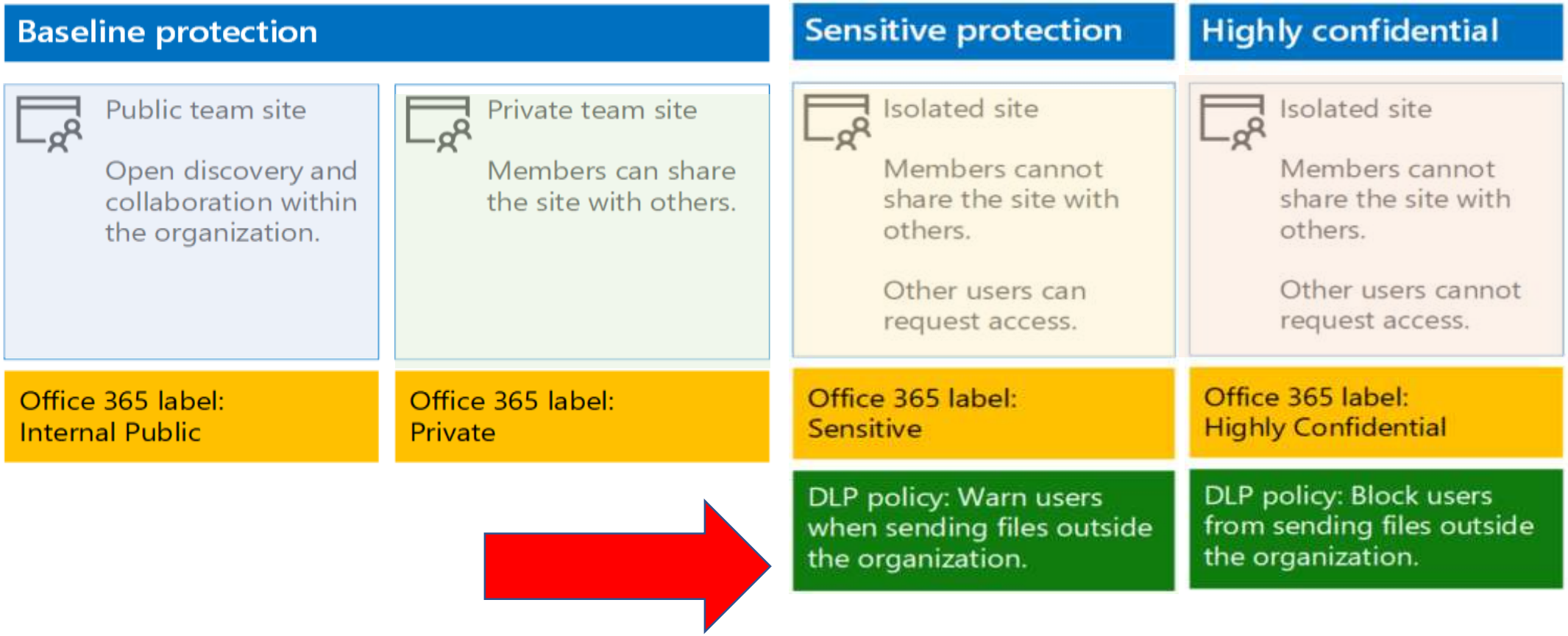
Office 365 E3 for manual labeling and Office 365 E5 for automated labeling. And for other locations, Azure Information Protection P1 for manual labeling and Azure Information Protection P2 for automated labeling

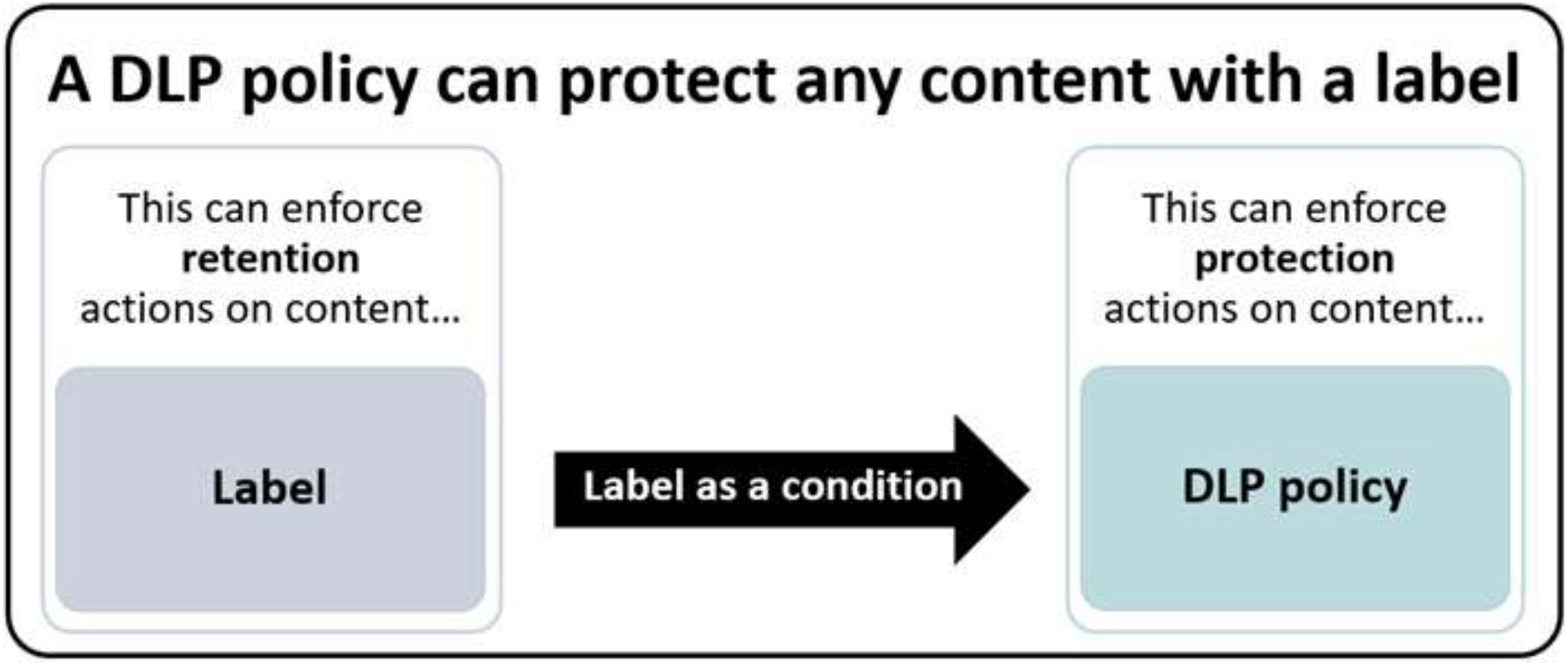
Step 3

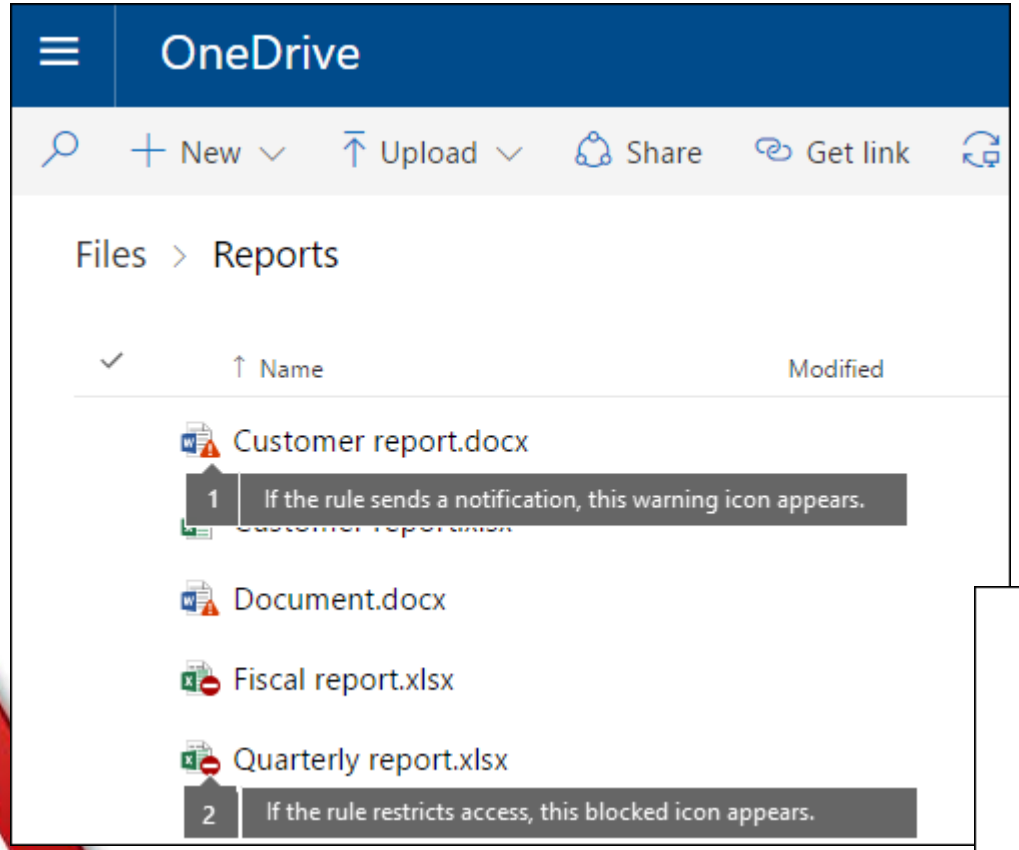
Create and Apply DLP Policies to Warn and Block

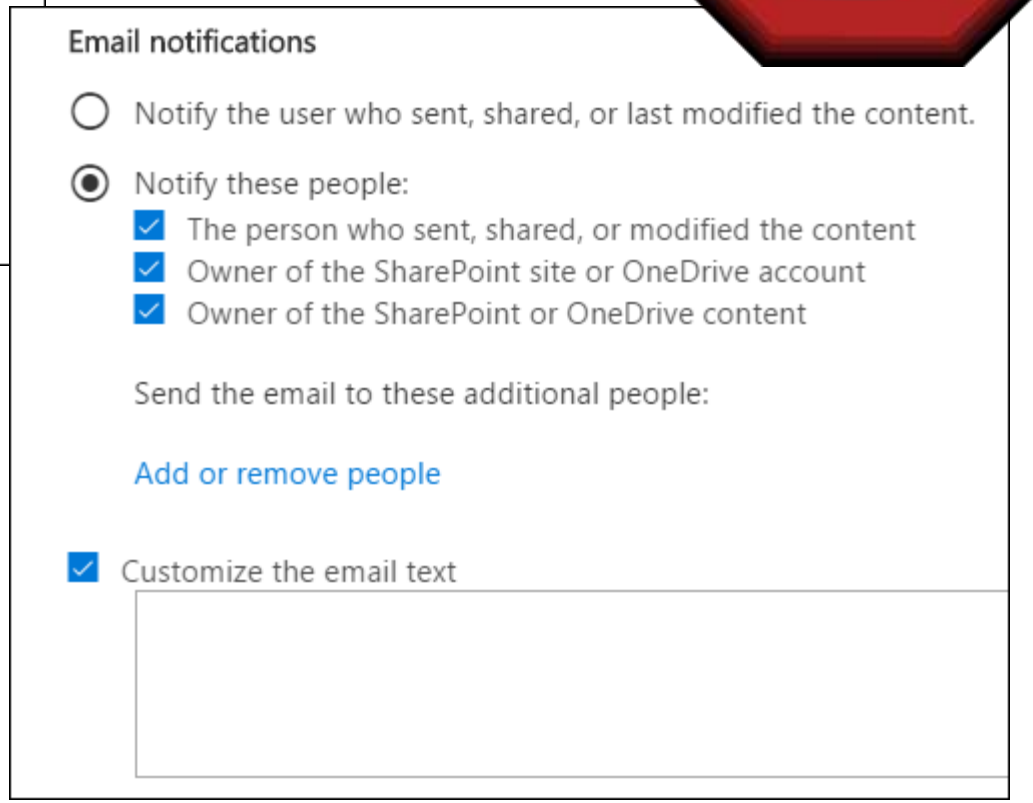
DEMO Part 2: Information Protection in Office 365 and DLP Reporting

Create & Apply DLP Policies to Block and Warn Users




A DLP policy can protect any content with a label
This can enforce
retention
actions on content...
Label
Label as a condition
This can enforce
protection
actions on content...
DLP policy


OneDrive
New
Upload
Share
Get link
Files
Reports
Name
Modified
Customer report.docx
1
If the rule sends a notification, this warning icon appears.
Document.docx
Fiscal report.xlsx
Quarterly report.xlsx
2
If the rule restricts access, this blocked icon appears.


Email notifications
Notify the user who sent, shared, or last modified the content.
Notify these people:
The person who sent, shared, or modified the content
Owner of the SharePoint site or OneDrive account
Owner of the SharePoint or OneDrive content
Send the email to these additional people:
Add or remove people
Customize the email text

Icons in Labeling and Enforcement


Malware


DLP warning


Personal checkout


Trending


Other checkout


Record


Missing metadata


“New”


DLP blocked


Shared

Users Save and Classify Files Direct from SharePoint online

Step 4

If you build it, Will they come?

Colligo – Bridging The Usability Gap

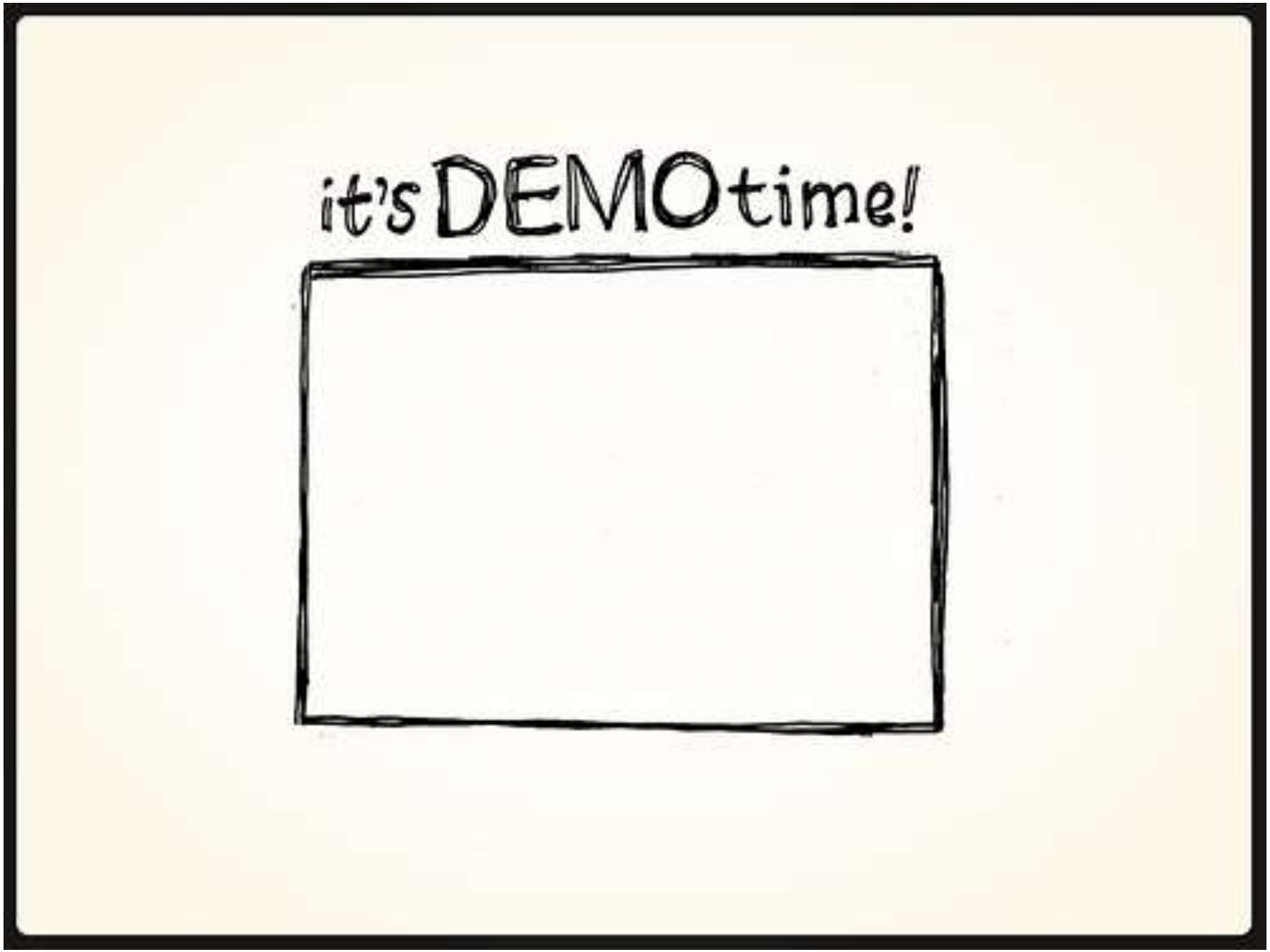
Usability barriers for users

- Their priority is productivity today - don't have time to jump complex hoops to get files properly classified in SharePoint
- Do not care much about Record Manager Priorities
- Primarily work in Outlook and Office, not SharePoint

Gaps Bridged by Colligo Add-ins

- Quickly save files to Pinned SharePoint locations without leaving Office
- Apply retention labels and other metadata in one intuitive flow (defaults by location)
- Retrieve documents from SharePoint inside Office for updating or sharing
- Available where users work: Desktop, Web, and Mobile Outlook

colligo



Office Add-In Benefits

- Not your father's add-in - not based on VSTO COM technology – based on Web Technology
- Centralize Deployment (5 minutes) - No desktop install
- Easily extends Office' functionality
- Cross-Platform: Run wherever you run Office: Windows, Mac, Web Browser, iPhone/iPad, Android
- No IT work to upgrade Add-in

https://docs.microsoft.com/en-us/office/dev/add-ins/overview/office-add-ins

Resources

- Protect SharePoint Online Files with Labels and DLP https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp
- Overview of Sensitivity Labels https://docs.microsoft.com/en-us/office365/securitycompliance/sensitivity-labels
- Overview of Labels https://docs.microsoft.com/en-us/office365/securitycompliance/labels
- Enable Site Classification in your tenant https://docs.microsoft.com/en-us/sharepoint/dev/solution-guidance/modern-experience-site-classification
- Office Add-ins Overview https://docs.microsoft.com/en-us/office/dev/add-ins/overview/office-add-ins

Q&A Discussion

- Webinar recording will be emailed to you within 24 hours.
- Enter questions in the Control Panel

Joel Oleson

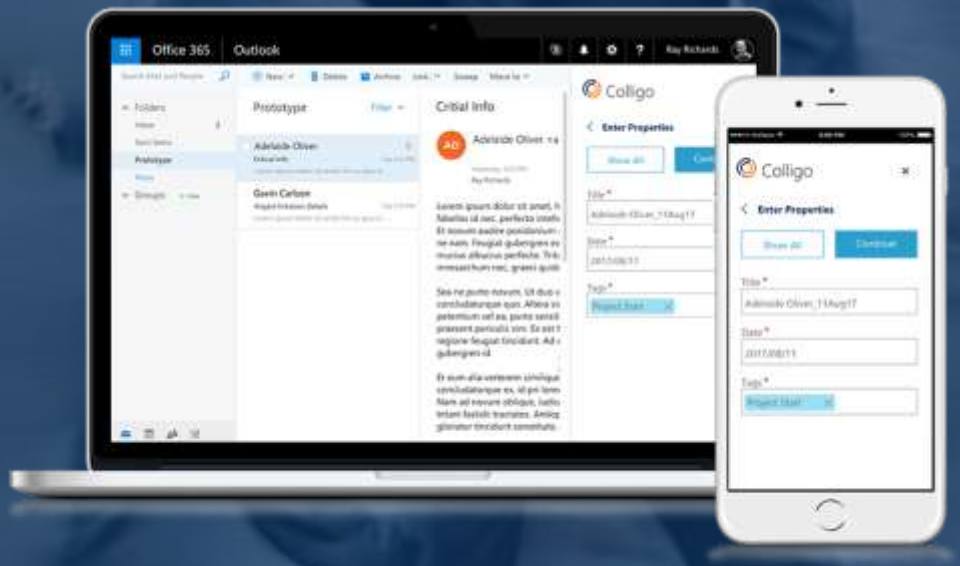
Office Apps & Services MVP

@joeloleson

collabshow.com

Roland Reddekop

Presale Engineer, Colligo



To request a demo go to:

colligo.com

Appendix

colligo

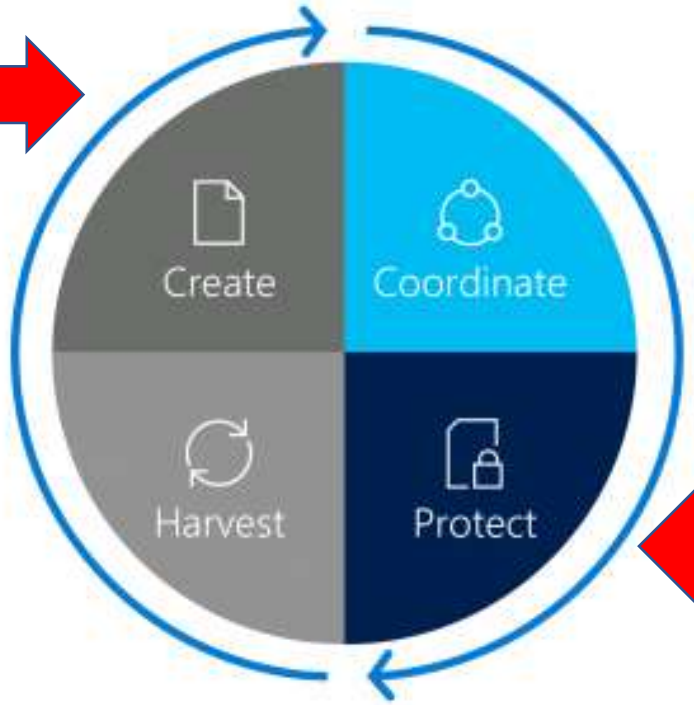
Microsoft Modern Content Management

The FOUR PILLARS of content services:

Create

Manage documents from the **moment** they're created or received

- Publish content to Shared and Protected Repositories
- Content type
- Metadata
- Apply O365 Labels



Protect

Manage compliance and reduce risk with information lifecycle governance

- Sensitivity labels
- Retention labels

Office 365 Labels

https://resources.techcommunity.microsoft.com/content-services/

Colligo Office Add-Ins for Office 365

E-Mail Manager for Office 365

- **Apps:** Outlook
- **Platform:** Windows/Mac/Online/Mobile
- **Function:** Manage key emailed content in SharePoint

Document Manager for Office 365

- **Apps:** Word, Excel, PowerPoint
- **Platform:** Windows/Mac/Online
- **Function:** Manage documents in SharePoint from the moment they're created

Workflow

1. Choose SharePoint Location
2. Apply Metadata & Labels
3. Search, Update & Share Content

Four Phased Approach for Protect SharePoint Online Files with Labels and DLP

Step 1: Determine the Office 365 labels

Four levels of information protection: Recommended Levels and Labels

SharePoint Site Level		Label name
Baseline	Public	Internal public
Baseline	Private	Private
Sensitive Protection		Sensitive
Highly Confidential		Highly Confidential

Step 2: Create, Publish and Apply Office 365 labels to libraries

1. Create the labels, you can use the Office 365 Admin center or Microsoft PowerShell:
$labelNames=@(<list of label names, each enclosed in quotes and separated by commas>)
ForEach ($element in $labelNames){ New-ComplianceTag -Name $element }

2. Publish your new labels
Home > Labels pane of the Security & Compliance Center, click the **Retention** tab, and then click **Publish labels**.

3. Apply the Office 365 labels to the documents libraries of your SharePoint sites.
Go to Documents >Library settings> Permissions and Management > **Apply label to items in this library** > **Settings-Apply Label**, select the label > **Save and Repeat.**

Step 3: Create and Apply DLP Policies to Warn or Block

1. Create DLP Policy go to **Security & Compliance** tab in your browser, click **Data loss prevention > Policy**.
In the **Data loss prevention** pane, click **Create a policy**.
2. For Sensitive setup Warn DLP Policy
3. For Highly Confidential setup Block DLP Policy

Step 4. Easily Save emails and files directly to SharePoint Online

Joel Oleson @joeloleson
Office Apps & Services MVP
Regional Director

Microsoft References:

https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp

Sponsored by: colligo

Phase 2: Create the Office 365 labels

- Sign in to the Office 365 portal with an account that has the Security Administrator or Company Administrator role. For help, see Where to sign in to Office 365.
- From the **Microsoft Office Home** tab, click the **Admin** tile.
- From the new **Office Admin center** tab of your browser, click **Admin centers > Security & Compliance**.
- From the new **Home - Security & Compliance** tab of your browser, click **Classifications > Labels**.
- From the **Home > Labels** pane, click the **Retention** tab, and then click **Create a label**.
- On the **Name your label** pane, type the name of the label and a description for admins and users, and then click **Next**.
- On the **Label settings** pane, click **Next**.
- On the **Review your settings** pane, click **Create**, and then click **Close**.
- Repeat steps 5-8 for your additional labels.

Publish your new labels

- From the **Home > Labels** pane of the Security & Compliance Center, click the **Retention** tab, and then click **Publish labels**.
- On the **Choose labels to publish** pane, click **Choose labels to publish**.
- On the **Choose labels** pane, click **Add** and select all four labels.
- Click **Done**.
- On the **Choose labels to publish** pane, click **Next**.
- On the **Choose locations** pane, click **Next**.
- On the **Name your policy** pane, type a name for your set of labels in **Name**, and then click **Next**.
- On the **Review your settings** pane, click **Publish labels**, and then click **Close**.

Enforce DLP Policies on your SharePoint sites

- From the **Microsoft Office Home** tab, click the **Admin** tile.
- From the new **Office Admin center** tab of your browser, click **Admin centers > Security & Compliance**.
- On the new **Security & Compliance** tab in your browser, click **Data loss prevention > Policy**.
- In the **Data loss prevention** pane, click **+ Create a policy**.
- In the **Start with a template or create a custom policy** pane, click **Custom**, and then click **Next**.
- In the **Name your policy** pane, type the name for the sensitive level DLP policy in **Name**, and then click **Next**.
- In the **Choose locations** pane, click **Let me choose specific locations**, and then click **Next**.
- In the list of locations, disable the **Exchange email** and **OneDrive accounts** locations, and then click **Next**.
- In the **Customize the type of content you want to protect** pane, click **Edit**.
- In the **Choose the types of content to protect** pane, click **Add** in the drop-down box, and then click **Labels**.
- In the **Labels** pane, click **+ Add**, select the **Sensitive** label, click **Add**, and then click **Done**.
- In the **Choose the types of content to protect** pane, click **Save**.
- In the **Customize the type of content you want to protect** pane, click **Next**.
- In the **What do you want to do if we detect sensitive info?** pane, click **Customize the tip and email**.
- In the **Customize policy tips and email notifications** pane, click **Customize the policy tip text**.
- In the text box, type or paste in one of the following tips, depending on if you implemented Azure Information Protection to protect highly confidential files:
- To share with a user outside the organization, download the file and then open it. Click File, then Protect Document, and then Encrypt with Password, and then specify a strong password. Send the password in a separate email or other means of communication.
- Highly confidential files are protected with encryption. Only external users who are granted permissions to these files by your IT department can read them.
- Alternately, type or paste in your own policy tip that instructs users on how to share a file outside your organization.
- Click **OK**.
- In the **What do you want to do if we detect sensitive info?** pane, click **Next**.
- In the **Do you want to turn on the policy or test things out first?** pane, click **Yes, turn it on right away**, and then click **Next**.
- In the **Review your settings** pane, click **Create**, and then click **Close**.