

# Safe Sharing with Purview Information Protection and the Traffic Light Protocol

September 17, 2024

11 - 11:45 AM EDT

# Peter Carson



- President, Extranet User Manager and Envision IT
- 14-time Microsoft M365 MVP
- [pcarson@envisionit.com](mailto:pcarson@envisionit.com)
- [blog.petercarson.ca](http://blog.petercarson.ca)
- President, Toronto Microsoft 365 User Group



# 3 Key Takeaways

1

Sharing will happen but will it be safe?

2

Microsoft 365, properly configured, can be both secure and simple

3

Start small and build from there

## About Us

---

- Established in 2008 in Toronto, Canada area
- Brand of software products owned by Envision IT Inc.
- Leader in the Microsoft 365 space and a Microsoft Partner for 10+ years



# Extranet User Manager

## We Make Microsoft Simple

---

- We make Microsoft simple for organizations to connect with their external stakeholders
- An exceptional user experience lets businesses collaborate with external stakeholders and maintain Microsoft security.
- IT is involved at the beginning, ensuring a seamless integration, while the business can focus on what really matters – **getting the job done.**

# Agenda

- Introductions
- Sharing challenges
- Microsoft Purview
- Traffic Light Protocol
- Implementation
- Summary, Q&A and Closing

# The Hidden Costs of Insecure Sharing



**Data Loss**



**Financial Drain  
from Shadow IT**



**Cyber Attacks**



**Underutilized  
Microsoft 365  
Investments**



**Process Management  
Inefficiencies**

# The Choices for 'Under the Radar' Sharing are Endless





# Why Microsoft 365?

- It's the place your employees are already working
- Users are more likely to use platforms they already understand and trust
- Robust security features, with continuous investment in state-of-the-art cybersecurity measures.
- Extensive compliance certifications



# Sharing Options in Microsoft 365

## Open

- Wild West
- Anything goes
- Oversharing

## Turn off all sharing

- Expect lots of Shadow IT
- Email attachments

## Purview

- Proper governance
- Policies define sharing by sensitivity

# Microsoft Purview

- **Unified Data Governance:** Provides a comprehensive platform for data governance across hybrid and multi-cloud environments.
- **Data Discovery & Classification:** Enables automated scanning, classification, and cataloging of data assets.
- **Integration:** Seamlessly integrates with Azure Synapse, Power BI, and Microsoft 365 for enhanced governance capabilities.
- **Compliance & Security:** Helps organizations meet compliance requirements and protect sensitive data through features like data loss prevention, eDiscovery, and risk management.



# Purview Labels

## Retention

- Manage lifecycle of data
- Specify how long content should be kept and then what actions should be taken
- Ensure compliance with regulations and internal policies
- Typically many (could be hundreds) of labels

## Sensitivity

- Designed to protect sensitive information
- Classifying and secure
- Control how content is handled and shared
- Small number of labels

# Microsoft Purview Information Protection

- Discover, classify, and protect sensitive data
- Data Discovery
  - Identify and classify sensitive data
  - On-premises, in the cloud, or in hybrid environments
- Sensitivity Labels
  - Apply labels to data to enforce protection policies like encryption, access restrictions, and visual markings
- Data Loss Prevention (DLP)
  - Prevent data breaches by using DLP policies to monitor and control the sharing of sensitive information
- AI-Powered Classifiers
  - Use AI to accurately classify data based on content and context, enhancing the precision of data protection measures



# Purview Licensing Recommendations



Microsoft licensing is never a simple topic, and Purview is no exception. A few good resources to help navigate this are:

[Microsoft Compliance and Information Protection Licensing Guide](#)

[All About Microsoft Purview Sensitivity Labels](#)

[Microsoft 365 Licensing](#)



The simple version: users require E3 or above to apply a label manually, while automatic policy-driven application of labels requires E5

Microsoft 365 E3 or E5 compliance licenses can be added to other licenses

# Copilot Readiness



## Permissions

Oversharing is common  
Copilot will incorporate any content you have access to  
Permissions review is key prior to launching Copilot



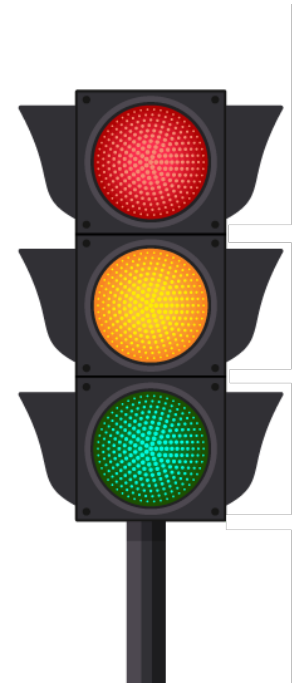
## Sensitivity

Without labeling Copilot doesn't know the sensitivity of content it is using  
Users need to be informed if sensitive content is incorporated in their generated content

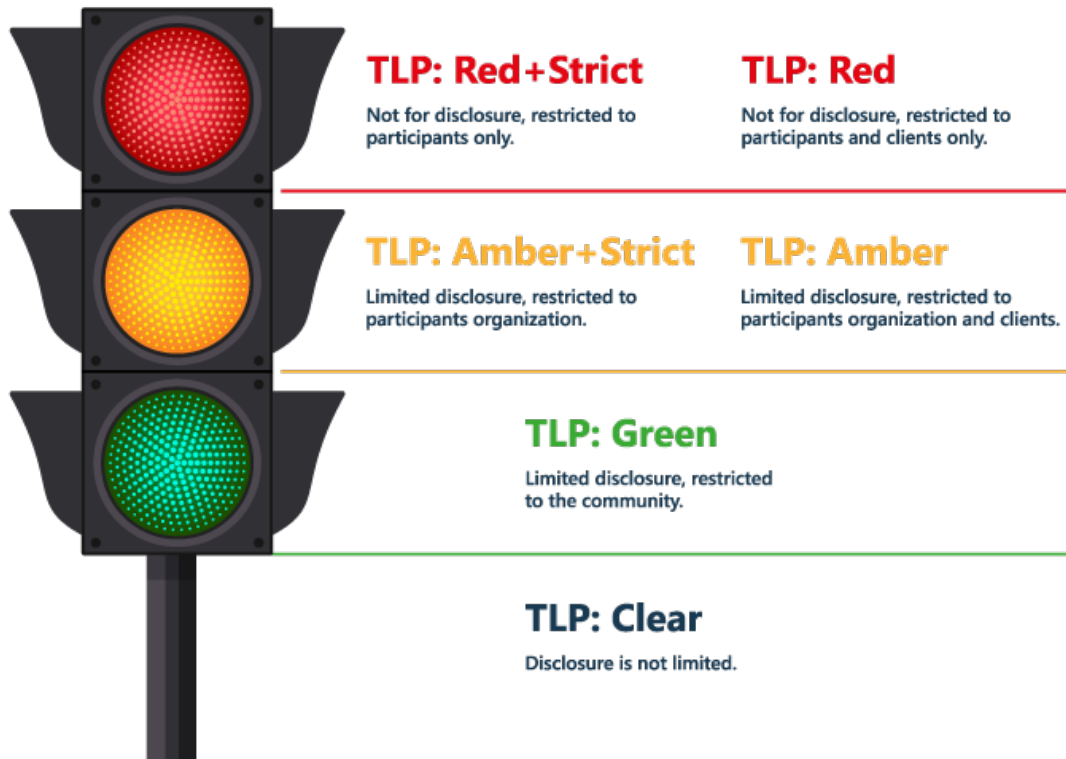
# Traffic Light Protocol: Simplifying Sensitivity Labels in Microsoft 365

The **Traffic Light Protocol (TLP)** is a classification system that uses color-coded labels to categorize and control the sharing of sensitive information.

- Developed by the UK's National Infrastructure Security Coordination Centre in the early 2000s
- Encourages sharing of sensitive information
- Adopted by the US Cybersecurity and Infrastructure Security Agency (CISA)
- Not a technical solution and not part of Purview



# TLP Labels and their Meanings



- **Red:** Most sensitive information; requires MFA and document encryption
- **Amber:** Sensitive information; external sharing allowed with MFA
- **Green:** Less sensitive; accessible to guests without MFA
- **Clear:** Public information; accessible without restrictions



# TLP and External Access in Microsoft

## 365

Below is a suggested implementation of TLP for defining guest access in Microsoft 365:

TLP	External Access	Guests Require MFA	Document Encryption	M365 Member Licensing
Red+Strict	No	N/A	Yes	E5
Red	Yes	Yes	Yes	E5
Amber+Strict	No	N/A	No	E3
Amber	Yes	Yes	No	E3
Green	Yes	No	No	E3
Clear	Yes	No	No	N/A

# TLP Green



- Low sensitivity content
- Can be shared externally
- No MFA requirement for external guests

# TLP Amber



- Medium sensitivity content
- Can be shared externally
- External guests require MFA
- Strict doesn't allow external sharing

# TLP Red



- High sensitivity content
- Can be shared externally
- External guests require MFA
- Office and PDF documents are encrypted
- Strict doesn't allow external sharing

# Benefits of TLP in Microsoft 365



Secure external sharing with appropriate MFA and encryption

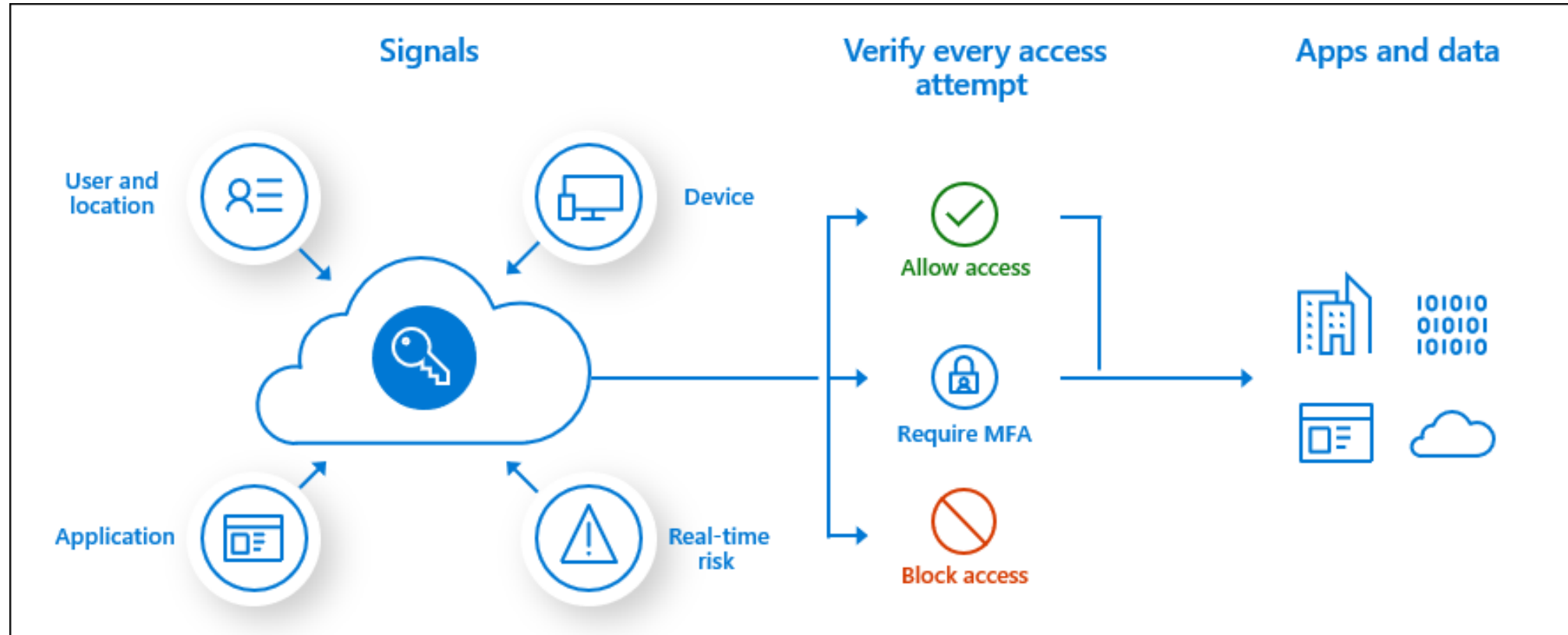


Clear, consistent classification for sensitive data



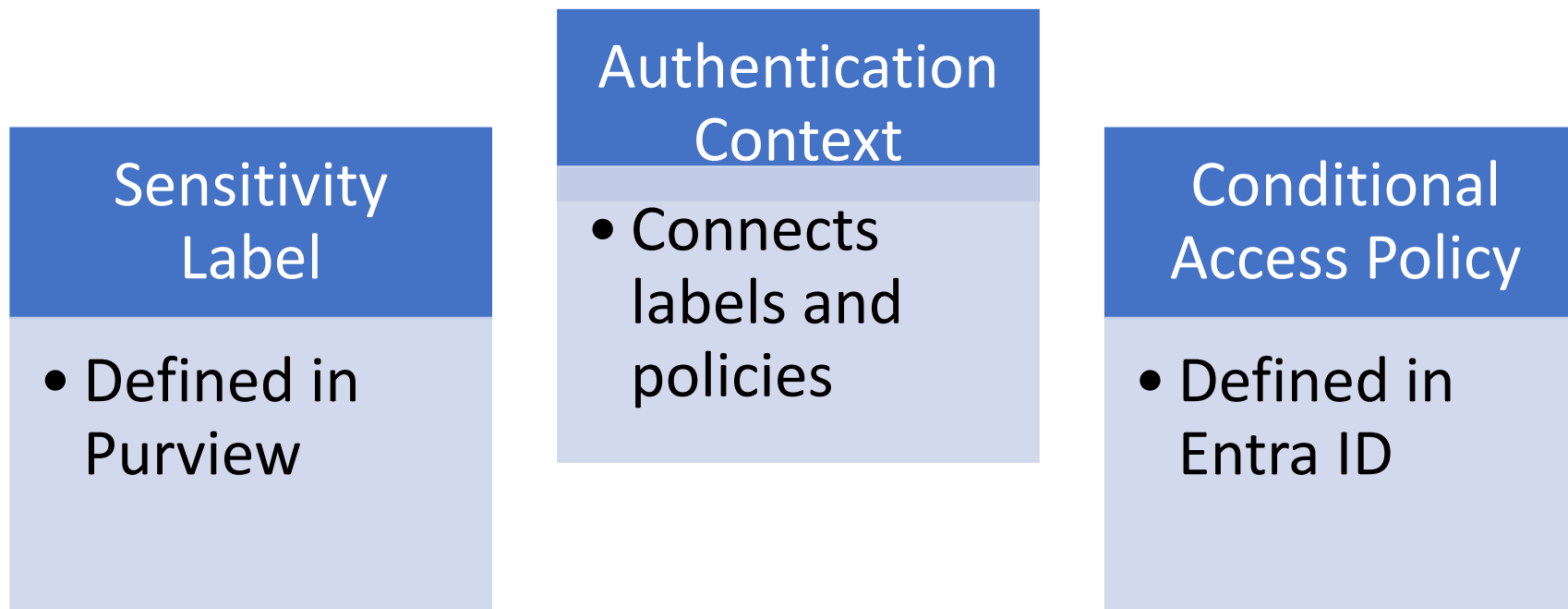
Enhanced governance and protection via Microsoft Purview

# Conditional Access Policies

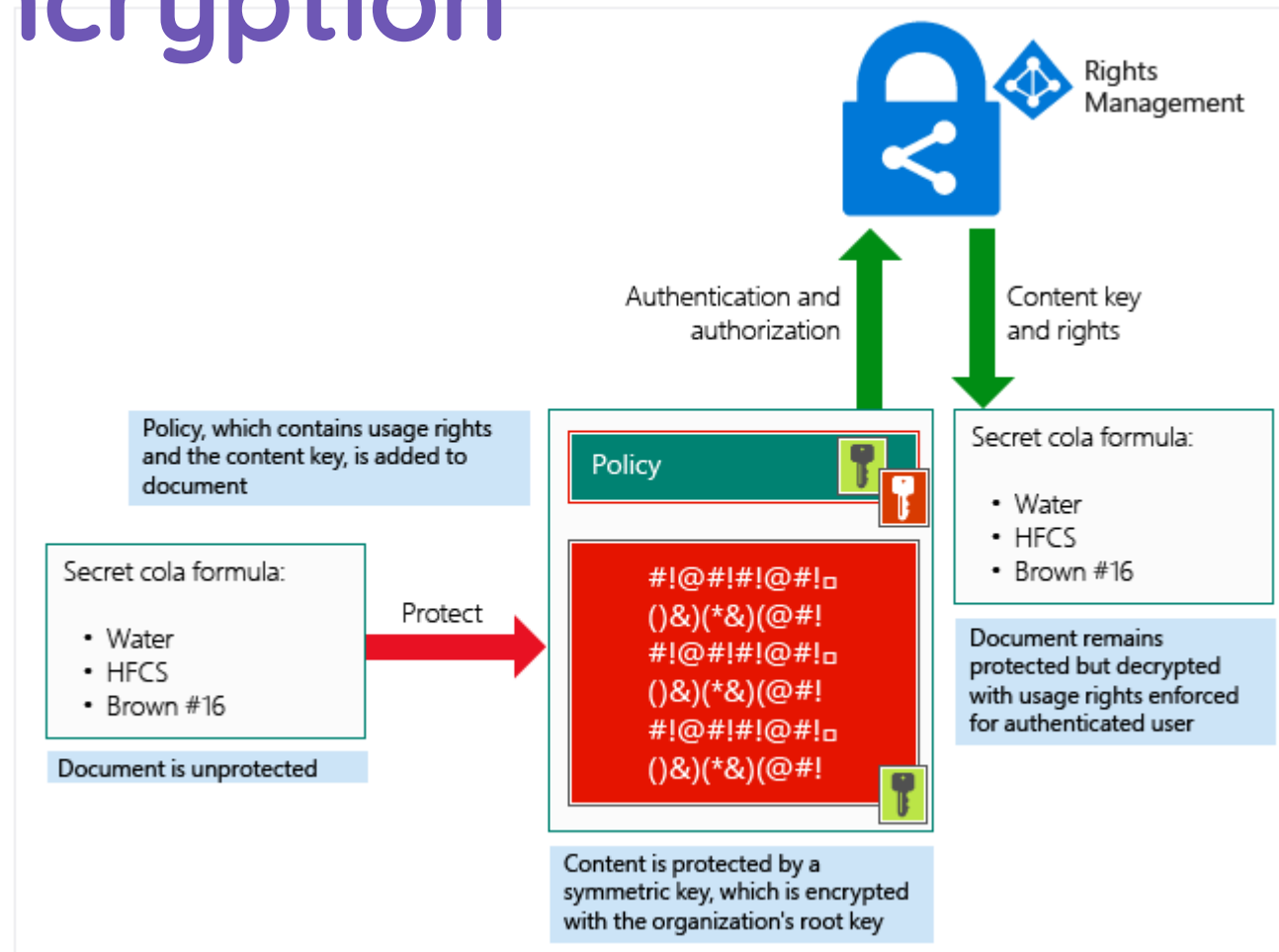


[Set up Microsoft Entra Conditional Access | Microsoft Learn](#)

# Authentication Context



# Data Encryption









[How Azure RMS works - Azure Information Protection | Microsoft Learn](#)



# Phase One Implementation of Purview

1. Define Container Labels  Create Green and Amber labels in Purview for SharePoint sites and containers, setting rules to determine external access and MFA requirements.
2. Establish Authentication Contexts  Set specific authentication contexts for each label to ensure appropriate security checks like multi-factor authentication are enforced for external users.
3. Build Conditional Access Policies  Create policies that apply the correct access control based on membership and guest status.
4. Inventory and Label Existing Sites  Audit current SharePoint and Teams sites, applying appropriate labels based on their sensitivity.

# Phase Two Implementation of Purview

1. Define Content Labels  Extend TLP sensitivity labels to individual documents by configuring Purview to recognize and protect highly sensitive content.
2. Apply Access Controls & Document Marking  Configure Azure Information Protection and Rights Management to enforce encryption and granular permissions.
3. Set Default Label Rules  Link document labels to container-level labels, ensuring documents inherit sensitivity levels from the SharePoint site or container they reside in.
4. Configure Azure Services  Set up Azure Information Protection and Rights Management for automatic labeling and encryption of Red-level documents.
5. Auto-Labeling  Enable automatic labeling based on predefined conditions, using E5 licensing for consistent protection.
6. Implement Add'l Authentication Contexts  Add further conditional access policies to provide secure external access and MFA based on sensitivity.

# Midsize Ontario City

## Large Scale M365 Implementation

- Governance Solution for Teams/SP
  - Proliferation of Ad Hoc Teams and SP Sites
  - Leverage Properly Defined SP & Teams Structure
- Migration into New Structure
  - Multiple Meetings with large number of groups for planning purposes
  - Actual Migration

## Teams First IA

- Logical organization of Content
- Intuitive Navigation, Search
- Teams, Hub sites, SharePoint

## Adoption & Governance

- Orchestry for M365 Adoption and Governance
- Templates, Provisioning
- Self-service
- End-to-end lifecycle Management
  - Templates
  - Approvals
  - Policies for Naming Conventions
  - Archiving
- Policy Enforcement
- User Management

# Federal / Provincial / Municipal Agency

## Large Scale ECM Implementation

- Previously completed ECM Strategy engagement
- Defined new modern IA
- Migration into New Structure
  - Multiple Meetings with large number of groups for planning purposes
  - Actual Migration

## Purview Implementation

- Information Protection Workshop
- Configuration of Microsoft Purview sensitivity labels
- Entra ID Authentication Contexts and Conditional Access Policies
- Rights Management for document encryption and watermarking
- External sharing strategy and information architecture
- EUM Data Room POC with trial license

## Adoption & Governance

- Orchestra for M365 Adoption and Governance
- Templates, Provisioning
- Self-service
- End-to-end lifecycle Management
  - Templates
  - Approvals
  - Policies for Naming Conventions
  - Archiving
- Policy Enforcement
- User Management

# Provincial Healthcare Agency

## SharePoint Online Migration

- 19 SharePoint on premises farms 2010 through 2016
- Migrating into SharePoint Online
- Including Forms and Workflows
- All farms have been independently managed
  - Migration into New Structure
    - Multiple Meetings with large number of groups for planning purposes
    - Actual Migration

## Purview Implementation

- Already had sensitivity labels established
- Setting up authentication contexts
- Conditional Access Policies
- eDiscovery

## Members Portal

- Migrated off SharePoint 2013 to SharePoint Online
- Users were created as cloud only guest accounts
- SharePoint Online Communication Sites
- EUM Product used for user management
  - Leads are able to manage their own users

# Purview Information Protection Workshop

- 2 hr workshop led by Envision IT Principal Consultant
- Learn about:
  - Intro to Purview Information Protection
  - Identify and create sensitive information types
  - Create sensitivity labels following the Traffic Light Protocol approach and use auto-labeling policies based on these labels
  - Intro to authentication contexts and conditional access policies
  - Intro to DLP



# Power BI Microsoft 365 Dashboard



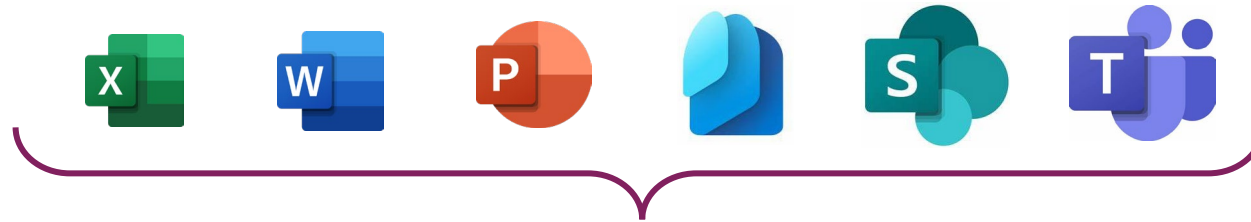
# Envision IT Purview Information Protection Engagement

- Licensing and tenant setup review and recommendations
- Information Protection Workshop
- Configuration of Microsoft Purview:
  - Sensitivity labels
  - Entra ID Authentication Contexts and Conditional Access Policies
  - Rights Management for document encryption and watermarking
  - Microsoft 365, Teams, and SharePoint configuration
- External sharing strategy and information architecture



# EUM Data Room

The EUM Data Room is a secure digital resource that the business finds easy to use and allows IT and Compliance to sleep well at night. Built on enterprise class Microsoft security, all your data stays in Microsoft 365 tenant and retains your brand throughout.



Document Type	Required	Instructions
Agenda		Latest monthly
Notes		

Document Type	Document	Modified
Trial Balance	Bulletin	2023-11-01, 4:17:04 p.m.
P&L	Bulletin	2023-10-28, 10:40:03 p.m.
Fin.	Change Requests.docx	2023-10-28, 10:40:03 p.m.
P&L	Closing Report.docx	2023-11-02, 9:54:17 a.m.
Financial Statement	Communications Plan.docx	2023-11-02, 9:54:20 p.m.
Financial Statement	trial.docx	2023-11-29, 10:10:11 a.m.

**Data Room Loan Application**

Status: New

Loan Amount: \$50,000.00

Document Type	Required	Instructions
Other		
Blind Tuning	Yes	
Peter Demo	Yes	
Peter Demo 2		

Document Type	Document	Modified
Financial Statement	Bulletin.pdf	2023-11-28, 8:00:35 a.m.
Financial Statement	Change Requests.docx	2023-11-25, 7:41:11 a.m.
P&L	Closing Report.docx	2023-11-25, 7:41:11 a.m.
Trial Balance	Communications Plan.docx	2023-11-25, 7:41:10 a.m.

**Data Room Simple Contribute**

Document	Modified
Change Requests.docx	2023-11-25, 7:41:11 a.m.
Communications Plan.docx	2023-11-25, 7:41:10 a.m.

Document	Modified
trial.docx	2023-11-29, 10:10:11 a.m.
trial.docx	2023-11-29, 10:10:11 a.m.
trial.docx	2023-11-29, 10:10:11 a.m.

# 3 Key Takeaways

1

Sharing will happen but will it be safe?

2

Microsoft 365, properly configured, can be both secure and simple

3

Start small and build from there

# Upcoming Events



## CollabDays Bletchley 2024

Bletchley, England  
Sep 25



## AI Community Conference

Vancouver, Canada  
Oct 18



## Azure AI Search and OpenAI Webinar

Online  
Oct 29

[Events | Extranet User Manager](#)

# Thank you!

Any Questions?