Information Security Practice:

Sensitivity Labels

Summary

UWM has implemented Sensitivity Labels in the Microsoft 365 environment, bolstering the campus community's ability to protect sensitive information from unauthorized disclosure, and improve privacy controls within the Microsoft environment.

Implementation Details

UWM's implementation of sensitivity labels includes two different label types: "Sensitive" and "Restricted". The Sensitive label is the less restrictive of the two, allowing individuals to share sensitive information with both UWM accounts and external guests, so long as they are authenticated. The Restricted label is stricter and will prevent files from being shared outside of the UWM community. Authentication is required to access files or emails that have either label applied, with Restricted labels being further restrained to only UWM staff that have been allocated access by the file owner.

Labels are applied in two different ways, one through an 'auto-labeling' feature, wherein Microsoft will passively scan all files in the OneDrive, Teams, SharePoint, and Outlook environments for 'sensitive information types'. The sensitive information types that Microsoft automatically detects include U.S. bank account number, U.S. driver's license number, U.S. social security number (SSN), U.S./U.K. passport number, and Credit Card Numbers. When these fields are identified, a 'Sensitive' label will automatically be applied to the document or email that generated the detection. This label provides the user with additional functionality to restrict sharing and manage access to the document or email.

The other way labels are applied is through manual configuration via the 'Sensitivity Bar' in Office documents and emails. Clients are empowered to apply labels to documents they deem as sensitive, with only a couple of clicks within the document itself. Individuals can also change labels to a less or more sensitive label type and can remove labels entirely - so long as justification for doing so is provided. The following Microsoft link contains how-to information for applying sensitivity labels within Office documents: Microsoft Sensitivity Labels - Client-Side Information.

Microsoft maintains a list of known issues and workarounds (Updated 8/21/23). If you encounter an issue with the sensitivity labels, please refer to the following document.
https://support.microsoft.com/en-us/office/known-issues-with-sensitivity-labels-in-office-b169d687-2bbd-4e21-a440-7da1b2743edc

If your issue is not found in the preceding document, please submit a support request here: https://uwm-amc.ivanticloud.com/Modules/SelfService/#globalHome

Label Best Practices

Sensitive

The Sensitive label is the less constraining of the two labels and is the default label applied by Microsoft's auto-labeling engine when high-risk data types are detected in files and email. The datatypes detected by the auto-labeling engine include U.S. bank account number, U.S. driver's license number, U.S. social security number (SSN), U.S./U.K. passport number, and Credit Card Numbers. Files that contain medium or high-risk data types, as outlined under UWSA 1031.A, should have the sensitive label applied. Examples of information that meets these criteria include protected health information (PHI), FERPA data, personally identifiable data (PII), and contractually protected data, to name a few.

Restricted

The Restricted label is the more constraining of the two labels and should only be used for files and emails that are not intended to be shared outside of the UWM environment. The auto-labeling engine does not apply the Restricted label, which can only be applied manually by users within the file or email they want to label. Files containing high risk data, which is not intended to be shared outside of your team or organization should be labeled with the Restricted label. The Restricted label will prevent any form of external sharing. The Restricted label should be used situationally, depending on the needs of the individual or group that need to maintain the highest levels of privacy. Please consult with your manager or group leadership to determine when it is appropriate to apply these restrictions.

If you need more guidance on what labels to apply and when, please contact the Information Security Office for more information.