



**VANDERBILT UNIVERSITY**  
Office of Cybersecurity



## **Sensitivity Labeling in Microsoft Tools**



## Introduction

This guide will provide concise guidance for labeling sensitive file types in Microsoft tools. (e.g., Word, Excel, PowerPoint, etc.) The goal is to safeguard the security and privacy of Vanderbilt University's data while complying with legal standards.

This information applies to all Vanderbilt Students, Faculty, Staff, and other VU community members. The labeling of sensitive files can be used with many different Microsoft file types; this document focuses explicitly on the following:

### Desktop Applications

- Word
- Excel
- PowerPoint
- Outlook

### Web Applications

- Office 365 (Word, Excel, PowerPoint, Outlook)
- Teams
- SharePoint
- And mobile editions of these apps

**When to apply:** Users should apply Sensitivity labels to documents and emails during creation or modification. Label application is essential when the content contains confidential, proprietary, or personally identifiable information (PII) that requires protection to prevent unauthorized access, comply with regulatory standards, and mitigate potential data breaches.

**Why apply:** Applying sensitivity labels to Vanderbilt documents is fundamental to maintaining the integrity and security of our data. It ensures that sensitive information is consistently identified, classified, and protected across all platforms and storage locations. By labeling files, we enforce data handling policies, control access based on data classification levels, and facilitate secure sharing within and outside the organization. This practice supports our commitment to regulatory compliance, intellectual property protection, and privacy obligations.



**General Guidance**

1. The labeling of sensitive files is determined according to the [Data Classification Guidance](#), following Vanderbilt University's [Data Classification Policy](#), which is divided into four levels based on the criticality of the data. The table below highlights each level's key privacy and security settings for the corresponding data sensitivity label.

	Classification	Level 1	Level 2	Level 3	Level 4
		Public	Institutional Use Only	Restricted	Critical
<b>Encryption</b>	<b>Encryption Required?</b>	No	No	Yes	Yes
	<b>Offline Access Available?</b>	Always	30 Days	Never	Never
<b>Content Marking</b>	<b>Content Mark Required?</b>	No	No	Header Only	Header and Content
<b>Privacy and External User Access</b>	<b>Privacy Expectation?</b>	None	None	Private	Private
	<b>External User Access Available?</b>	Yes	Yes	No	No
<b>External Sharing and Conditional Access</b>	<b>External Sharing from SharePoint?</b>	Anyone	Existing Guests	Existing Guests	Only Those in Your Org

2. Each Data Sensitivity label has embedded security and privacy settings consistent across various file types and platforms. The security and privacy settings become more restrictive as the data level increases.
3. Please contact [the Office of Cybersecurity](#) to request special Sensitivity labels that address unique data security and privacy needs.
4. Labeling every file with the appropriate level and applying labels consistently across similar types of documents is crucial.
5. Avoid classification errors by accurately applying sensitivity labels based on data sensitivity level. Under or over-classification can lead to exposing sensitive data or over-restricting unnecessarily.
6. Using different sensitivity labels for documents that change classification levels is recommended. For instance, when sensitive information is added or removed from a document.

## How to Apply Data Sensitivity Labels

When working with sensitive file types in Microsoft tools, there are specific icons that the user needs to identify to access the sensitivity labeling options. These buttons/icons resemble a rubber stamp on a piece of paper. They are available in both Classic and Simplified icon designs. Note that with

While using [desktop-based applications](#), look for the Classic design. Look for the Simplified icon for [web and mobile apps](#) with fewer UI elements.




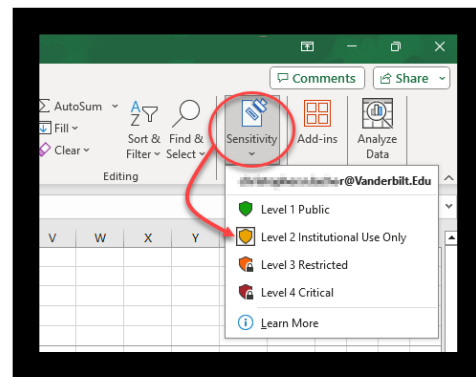
Classic Button



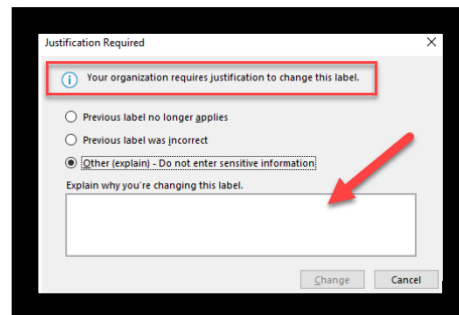
Simplified Icon

**Button Location:** To apply the label on most desktop applications, locate the Sensitivity icon on the Home tab on the far right-hand side of the toolbar.

For mobile apps, Sensitivity labeling settings will be located under Settings, aka - ellipsis icon. 



**Updating Label:** When changing sensitivity labels, the user must provide a justification reason. A message requesting the reason will pop up for the user to select from a pre-defined list or enter a new one.






## FAQs

### Microsoft Mobile Apps

#### Can Sensitivity labels be applied within Microsoft Mobile Apps?

**Answer: Yes.** The Sensitivity labeling function is available for Outlook, Teams and Microsoft 365 (Office) - including Excel, Word, and PowerPoint files.

#### Where can I find the Sensitivity labeling options within Microsoft Mobile Apps?

**Answer:** Open the file on your phone with a Microsoft 365 App and select the function button  in the upper corner of your screen. File sensitivity labels can be applied on the Settings screen.

### Microsoft Outlook

#### How are Sensitivity labels applied to an Email in Outlook?

**Answer:** Sensitivity labels can only be applied to Outlook emails when creating a new email or replying to an email. Once an email is sent or received, no Sensitivity labels can be used or changed.

#### Can Sensitivity labels be applied to Outlook Calendar appointments?

**Answer: Yes.** Security and privacy settings for Outlook emails or calendar appointments will apply to their attachments, but attachments will not inherit the Sensitivity label.

This means that if you apply a Sensitivity label to an email that restricts access to its content for people outside of Vanderbilt, the attachments within that email will also be restricted.

But, if you download the attachments separately from the email, the security and privacy settings won't apply unless you manually apply a Sensitivity label to the individual attachments. If attachments have been downloaded (separate from the email), the security and privacy settings won't apply to that file unless the user manually applies a Sensitivity label.

## Microsoft SharePoint

### Can Sensitivity labels be applied to a SharePoint site?

**Answer: Yes.** It is important to note that only site owners can set Sensitivity labels. Teams and SharePoint Sensitivity labels only apply to how Teams and SharePoint space is shared and accessed. However, it does not enforce inheritance capabilities to files created in such spaces.

For example, a user can create a SharePoint page and label it as Level 4, but this SharePoint site can host Microsoft files with Sensitivity labels set at other levels.

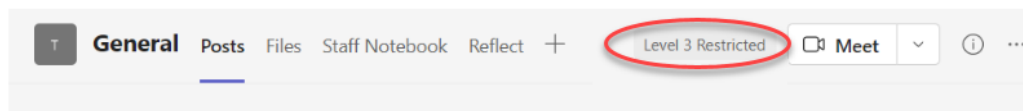
## Microsoft Teams

### Can Sensitivity labels be applied to new team (group/channel) in Teams?

**Answer: Yes.** Microsoft Teams Sensitivity labels can be set at creation. Vanderbilt preconfigured four types of Teams: Class, Professional Learning Community (PLC), Staff, and Other. But note that Sensitivity labels cannot be applied when starting a "Class" group. For all other Teams types, labels are available to be applied.

### Can Sensitivity labels be applied to existing teams (group/channel) in Teams?

**Answer: Yes.** To modify Sensitivity labels for an existing Team, users can go to "Edit team" in the Team settings function. After applying Sensitivity labels, the label will appear on the upper right corner of all Channels under the Team.



## Data Analytical Tools

### Can users still utilize analytical tools (PowerBI and Tableau) to access Excel files after Sensitivity labels have been applied?

**Answer: Yes. However, not for Level 3 or Level 4 files.** Vanderbilt Level 3 and Level 4 data Sensitivity labels enable encryption controls, which most data analytical tools don't allow the platform to connect with encrypted files.