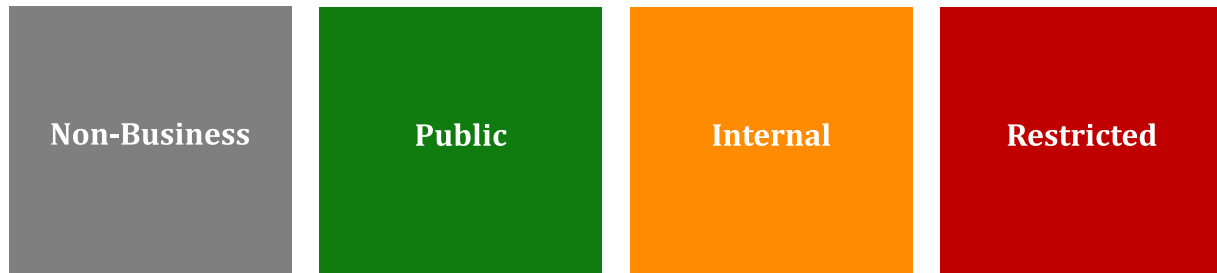


Ohio Christian University Sensitivity Label Definitions

Descriptions for each found below

- Non-Business
- Public
- Internal
- Restricted



Non-Business

Non-business data, for personal use only. Data that does not belong to OCU. Data is not encrypted and cannot be tracked or revoked. Do not use **Non-Business** to classify any data that belongs to OCU.

Use Cases for this label:

1. Writing an email (using your work provided device) to a friend and sharing photos from your last vacation
2. Planning a weekend getaway with your spouse and sharing the brochure over email
3. Writing a mail requesting updated car insurance rates.

Public

University data that's specifically prepared and approved for public consumption. Data is not encrypted and cannot be tracked or revoked.

Use Cases for this label:

1. Responding to someone about an OCU event
2. Links to publicly available blog articles, marketing videos, forum links
3. Sharing links to externally posted sites

Internal

Business Data which is NOT meant for public consumption. This includes sensitive business data that should not be shared with unauthorized people, but it can be shared with external partners as

needed. Examples include contracts, security reports, forecast summaries, and bank statements. This data should be encrypted if sent to external sources.

Use Cases for this label:

1. New Employee Orientation training content or email
2. Newsletter for the University
3. Email from OCU Senior Leadership Team on new compliance guidance

Use Cases for utilizing this label with external partners:

1. Emails with insurance agents (high level discussions). But once these discussions start getting into more confidential details, this should be labeled **Restricted**
2. New process for submitting expenses including sub-contractor travel
3. Discussions about network setup between IT and outside vendor

Restricted

Very sensitive data, such as student or employee personally identifiable information (SSNs, credit card numbers, passport numbers, HR records, medical information, etc.). This data is classified, encrypted, and protected. This information is restricted to only OCU employees except for rare cases and in those cases, it **MUST** always be encrypted before leaving the OCU network. As per GLBA, this data must be encrypted at rest as well as in transit (so always) unless it's actively being viewed.

Use Cases for this label:

1. Contacting Human Resources with a sensitive concern
2. Email from leadership on the upcoming quarterly performance and guidance
3. Discussions surrounding students or their data
4. Any documents or email that contain SSNs (or other personal information), credit card info, ABA info, or any other highly confidential information

Use Cases for utilizing this label with approved non-employees:

1. Financial Aid collecting sensitive data from students
2. Discussions between HR and potential employees/collection of forms and background information
3. Delivering student data or lists to DOE or accrediting agencies