# Data Classification and Handling

## 1. PURPOSE:

Information is a valuable College asset and is critical to the mission of teaching, research, and service to Thiel.

Determining how to protect and handle information depends on a consideration of the information's type, importance, and usage.

Classification is necessary to understand which security practices should be used to protect different types of information. The more protected the information needs to be, the more practices are required.

## 2. APPLIES TO:

College employees (faculty, staff, student employees) and other covered individuals (e.g., affiliates, vendors, independent contractors, etc.) in their handling of College data, information, and records in any form (paper, digital text, image, audio, video, microfilm, etc.) during the course of conducting College business (administrative, financial, teaching, research, or service).

"Handling" information includes, but is not limited to, the following: creating, collecting, accessing, viewing, using, storing, transferring, mailing, managing, preserving, disposing, or destroying.

## 3. POLICY STATEMENT:

A. All College employees and other covered individuals are responsible for:

1. Understanding what constitutes Private or Public College information; and
2. Managing Private or Public College information in a manner consistent with the criticality of and the requirements for confidentiality associated with the data in any form (electronic, documentary, audio, video, etc.) throughout the entire information lifecycle (from creation through preservation or disposal).

B. **All College information** whether **at rest** (i.e., stored in databases, tables, email systems, file cabinets, desk drawers, etc.) or **in use** (i.e., being: processed by application systems, electronically transmitted, used in spreadsheets, or manually manipulated, etc.) **must be classified into one of the three data classification levels described in this policy by each unit or department that is the Custodian of Records for that information.**

1. **Determining classification level** should be done according to an assessment of the need for **Confidentiality** of the information.
   ***Confidentiality:*** *Access to information must be strictly limited to protect the College and individuals form loss.*

*Limiting access to authorized individuals/entities/devices ensures legal obligations are fulfilled and/or protects Thiel and its stakeholders from the disclosure of data, which is sensitive in nature.*

**Note:** The appropriate classification of each data set is based on the classification of the most confidential data stored in the data set (e.g., the database, table, file, etc.), or accessed by systems or people. This is true even if the data set contains other information that would qualify for a lower level of protection if it were stored separately.

2. The table below summarizes the Data Classification process. All individuals covered under this policy are required to handle College information per the procedural controls found in this document.

| | |
|---|---|
| **Level I – Confidential Protection** | **STOP! SPECIAL CARE IS REQUIRED** |
| **Level II – Sensitive Protection** | **BE VERY CAUTIOUS** |
| **Level III – Public Protection** | **PROCEED WITH AWARENESS** |

- **Level I – Confidential Information:** High risk of significant financial loss, legal liability, public distrust, or harm if this data is disclosed.

Examples include:

- Data protected by HIPAA (health information)
- Data protected by FERPA (student information including grades, exams, rosters, official correspondence, financial aid, scholarship records, etc.)
- Data protected by GLB (financial information)
- Data subject to PCI (credit or payment card industry) standards
- Data subject to other Federal or state confidentiality laws
- Donor or prospect information
- Passwords and PINs
- Personally Identifiable Information (“PII”)
- Personnel data
- Individually identifiable information created and collected by research projects
- Certain research data with National Security implications
- Data subject to protection pursuant to non-disclosure agreements
- Audit working papers
- Data protected by attorney/client privilege
- Email covering topics listed above

- **Level II – Sensitive Information:** Moderate requirement for Confidentiality and/or moderate or limited risk of financial loss, legal liability, and public distrust, or harm if this data is disclosed.

  Examples include:
  - Audit reports
  - Email addresses that are not a public record
  - Other grants and contracts (not included above)
  - Competitive business information
  - System security information such as firewall rules and hardening procedures
  - Security incident information

- **Level III – Public Information:** Low requirement for Confidentiality [information is public] and/or low or insignificant risk of financial loss, legal liability, public distrust, or harm if this data is disclosed

  Examples include:
  - College directory information
  - Blogs
  - Web pages
  - Course offerings
  - Annual reports, etc.

**Approved Risk Level by Storage Category or Device**

| | **Approved Risk Level** | | | |
|---|---|---|---|---|
| **Service** | 1 | 2 | 3 | |
| Thiel College Own Workstations | ✓ | ✓ | ✓ | Level 2 and 3 data can be stored locally on your workstation. Level 1 data must be stored on CIS-approved secure centralized file shares or CIS-approved encrypted portable electronic storage devices. Level 1 data must be stored in ways explicitly designed and approved by CIS. |
| Personally Owned Workstations | | | ✓ | Personally owned workstations can only be used to store Level 3 data, that is, only Thiel College public information. |
| Active Directory-based Centralized File Share | ✓ | ✓ | ✓ | Work with CIS to establish an appropriate secure share for Level 1 data. |
| Office 365 - OneDrive | ✓ | ✓ | ✓ | Consult with CIS before using Office 365 – OneDrive storage for any new purpose to |

| | | | | |
|---|---|---|---|---|
| | | | | ensure proper security settings for shared O365 files and sites. |
| Office 365 – CIS Designed Share or Site | | ✓ | ✓ | CIS must explicitly design any O365 environment used to store Level 2 data. O365 provides sufficiently robust security for Level 2 data when appropriately configured and managed. |
| Email | | ✓ | ✓ | Never send Level 1 or higher data through email regardless of the email provider. Use an approved Office 365 share or an Active Directory-based centralized file share to share Level 1 or Level 2 data |
| Mobile Devices | | | ✓ | Mobile devices, whether Thiel College or personally-owned, may be used only with public, Level 3, Thiel College information. |
| Public Cloud Storage Sites (e.g. Box, Dropbox) | | | ✓ | Public Cloud storage other than approved O365 accounts may be used only for public information. |
| Portable Electronic Storage Media | | | ✓ | Never store Level 1, 2 or 3 data on portable electronic storage media such as USB devices, CD/DVD ROM, or external hard drives. |
| Encrypted Portable or Local Electronic Storage Media | ✓ | ✓ | ✓ | Work with CIS to design, acquire, and properly configure any encrypted portable or local storage environment. All storage for Level 1 data must be explicitly approved by the Director of Information Systems. |

## 4. EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

Exceptions to this Policy shall only be allowed if previously approved by the KU Information Technology Security Office and this approval is documented and verified by the Chief Information Officer.

## 5. CONSEQUENCES:

Faculty, staff, and student employees who violate this College policy may be subject to disciplinary action for misconduct and/or performance based on the administrative process appropriate to their employment.

Students who violate this College policy may be subject to proceedings for non-academic misconduct based on their student status.

Faculty, staff, student employees, and students may also be subject to the discontinuance of specified information technology services based on the policy violation.