THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0005 - Data Categorization	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure for the University to properly categorize the University's Data to ensure that the appropriate controls are in place to provide the most effective protections.

II. Categorization Policy

Each campus and institute must develop and maintain a formal documented program for the categorization of the University's Data including any Data that is processed or stored on University-owned Assets, Systems, or Resources, including Data stored on Information Technology Service Provider systems. Data from third parties in use by University personnel must be categorized as defined by the third party Data owner. The program must adhere to the following guidelines at a minimum. This includes training and communication about the program requirements that encourages engagement by the User community.

1. The Data Owner is responsible for categorizing the University Data that they are responsible for. The categorization information must be communicated to the Data Steward, the Data Custodian, the Data Users, and the Central IT Department.
2. **Data Confidentiality Categorization:** Data Owners will categorize the confidentiality of the University's Data based on the following (see paragraph III. for examples):
    a. Public (Level 0) – The effect on confidentiality of the Data is minimal. Data that would fit into this category includes that which by law is available to the public without request.
    b. Internal Use Only (Level 1) – The effect on confidentiality of the Data is significant but does not include compliance issues. This includes Data that is protected against unwarranted disclosure whose protection may be required for legal, ethical, or proprietary considerations.
    c. Private (Level 2) – The effect on confidentiality of the Data is significant and includes compliance requirements. This Data is governed by federal, or state compliance requirements and unwarranted exposure can lead to compliance issues and/or fines. This includes all Data that contains personally identifiable information (PII), protected health information, student education records, and card holder Data.
    d. Restricted (Level 3) – The effect on confidentiality of the Data is based on federal-government regulated research definitions and requirements regarding unwarranted exposure or related to control Systems that support the University, but if subverted, could be life-threatening to University Employees (Employee), students, and others using University facilities.
3. **Data Integrity Categorization:** Data Owners will categorize the integrity of the University's Data based on the following (see paragraph III for examples):

e. Level 0 – The effect on integrity of the Data is minimal. Data that would fit into this category includes Data that has no restriction on who can change it or when.

f. Level 1 – The effect on integrity of the Data is significant but does not include compliance issues. This includes Data that is protected against unwarranted change including Protected University Data whose protection may be required for legal, ethical, privacy, or proprietary considerations.

g. Level 2 – The effect on integrity of the Data is significant and includes compliance requirements. This Data is governed by federal, or state compliance requirements and unwarranted change can lead to compliance issues and/or fines. This includes, but is not limited to, all Data that contains personally identifiable information (PII), protected health information, student education records, and card holder Data.

h. Level 3 – The effect on integrity of the Data is focused on federal-government regulated research definitions and requirements regarding unwarranted change or is related to control Systems that support the University, but if subverted, could be life-threatening to University Employees, students, and others using University facilities.

4. Both confidentiality and integrity are evaluated and tracked individually and must be documented in a categorization inventory. If there are questions regarding the categorization, the Data and/or System owner must consult with the campus or institute's CISO/DISL. The security controls that are implemented for the protection of all the University's Data and Systems must be based on the categorization of the Data.

III. Pre-Defined Data Categorization Definitions

1. Any Data that has not been categorized by the Data Owner will be treated as Internal Use Only (Level 1) until it is properly categorized.

2. The following Data types are required to be categorized as Internal Use Only (Level 1). Other Data may be categorized as Internal Use Only (Level 1) based on the required protection requirements:

   a. Employee performance reviews

   b. Tennessee Unique ID

   c. Building floor plans showing egress routes and shelter areas

   d. Faculty tenure recommendations

   e. Data flow and IT Network infrastructure diagrams

3. The following Data types are required to be categorized as Private (Level 2). Other Data may be categorized as Private (Level 2) based on the required protection requirements:

a. Family Educational Rights and Privacy Act (FERPA)

b. Personally Identifiable Information (PII)

c. Donor contact information and non-public donation amounts

d. Sensitive Identifiable Human Subject Research Information (Human Subject)

e. General Data Protection Regulation (GDPR)

f. Personal Information Protection Law of the People's Republic of China (PIPL)

f. Social Security Number (SSN)

g. VISA numbers

h. Payment Card Industry (PCI) Data

i. Financial account numbers such as banking or investment account numbers

j. Protected Health Information (PHI) per the Health Insurance Portability and Accountability Act (HIPAA)

k. Biometric information

l. Gramm–Leach–Bliley Act (GLBA) Title IV loan Data

m. Trade secret or Intellectual Property protected by a non-disclosure agreement

n. Passwords, passphrases, PIN numbers, security codes, and access codes

4. The following Data types are required to be categorized as Restricted (Level 3). Other Data may be categorized as Restricted (Level 3) based on the protection requirements required:

   a. Controlled Unclassified Information (CUI)
   b. Export-Controlled Information (ITAR, EAR)

IV. Exceptions

The University's Chief Information Officer is authorized to grant exceptions to the University's Information Technology Policies. Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

SECTION 2. Reason for the Policy

This policy establishes the requirements for Data categorization for the University of Tennessee in support of System-wide Policy: IT0001 – General Statement on Information Technology Policy. All Users must familiarize themselves with System-wide Policy: IT0001.

SECTION 3. Scope and Application

This policy applies to all Users of IT Resources owned, operated, or provided by the University of Tennessee, including its campuses, institutes, and administration (University and/or campuses).

"Data" that is transmitted or stored on University IT Resources is the property of the University unless it is specifically identified in writing as the property of other parties. The University reserves the right to access the University's Resources and any non-University owned Resources that are or have been connected to the University's Resources or contain the University's Data.

Throughout this policy, it is understood that Users will not use personally licensed internet services (e.g., Google Mail, Google storage) for University business or store Protected University Data on a personally owned System.

SECTION 4. Procedures

Each campus/institute will adopt procedures to implement the controls necessary to adhere to this policy.

SECTION 5. Definitions

See IT0001 – General Statement on Information Technology Policy for definitions of terms.

SECTION 6. Penalties/Disciplinary Action for Non-Compliance

Any violation of this policy may subject the User to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct (HR0580 – Code of Conduct) in the Human Resources Policy and Procedures.

The University may temporarily or permanently remove access to its information technology Resources if an individual violates this policy.

SECTION 7. Responsible Official & Additional Contacts

Subject Matter	Office Name	Telephone Number	Email/Web Address
Policy Clarification and Interpretation	System Chief Information Officer and System Chief Information Security Officer	(865) 974-4810 or (865) 974-0637	cio@tennessee.edu or iso@tennessee.edu

Policy Training	System Chief Information Security Officer	(865) 974-0637	iso@tennessee.edu

---

SECTION 8. Policy History

Revision #:

SECTION 9. Related Policies/Guidance Documents

A. University Policies

a. IT0001 – General Statement on Information Technology Policy

b. IT0002 – Acceptable Use of Information Technology Resources

c. IT0003 – Information Technology Security Program Strategy

d. IT0004 – Information Technology Risk Management

e. IT0014 – Security Awareness Training Management

f. IT0017 – Information Technology Incident Response Management

g. IT0102 – Information Technology Asset Management

h. IT0311 – Information Technology Data Access, Management, and Recovery

i. IT0506 – Information Technology Account and Credential Management

j. IT1318 – Information Technology Network Monitoring and Defense and Penetration

k. IT1516 – Information Technology Service Provider Management Application Software Security Management

l. IT4912 – Information Technology Secure Configuration Management

m. IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense

B. Center for Internet Security Critical Security Controls Navigator

https://www.cisecurity.org/controls/cis-controls-navigator/

System-wide Policy: IT0005 - Data Categorization	
Version: 1	**Effective Date: 01/23/2025**