THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: IT0005-HSC-A Data & System Categorization	
Version 9	**Effective Date: 06/16/2020**

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

At the University of Tennessee Health Science Center (UTHSC), protecting our Institutional Information and IT Resources is critical to our teaching, research, clinical care, and public service mission.

This Standard defines requirements for appropriately categorizing Institutional Information and IT Resources to ensure confidentiality, integrity, and availability. It follows a risk-based approach to prescribe additional controls based on the need to achieve a specific level of protection for each category. UTHSC's investment in security controls is commensurate with the level of need for protection or availability of the Institutional Information

Scope

This policy applies to any form of data, including paper documents and digital data stored on any type of media and the systems or assets used to store, process, or transmit that data. It applies to all UTHSC employees and students, as well as to third-party agents authorized to access UTHSC data.

Definitions

Availability – ensuring timely and reliable access to, and use of, information.
Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
UTHSC Information Technology (IT) Resource - a broad term for all things related to information technology from a holistic point of view and covers all University-owned or managed information technology services, including cloud-based services, that users have access to.
Integrity – guarding against improper information modification or destruction and includes ensuring information accountability, non-repudiation, and authenticity.
Security Categorization - The process of determining the security category for data or an information system. Security categorization methodologies are described in Federal

Information Processing Standard (FIPS 199) and National Institute for Standards and Technology (NIST) SP 800-60. Security categorization helps identify the appropriate level of controls to be applied to the system or data.

Responsibilities

Data/System/Asset Owner — The owner is usually a senior stakeholder of a University asset/system and is responsible for ensuring that technology functions meet University goals and adhere to University policies and standards. The asset owner is ultimately responsible for ensuring the University security policies are followed and that risks associated with the asset/system are identified and managed to an acceptable level. The owner is ultimately responsible for the data and information being collected and maintained by their department or division. The owner shall address the following:

- **Review and inventory** — Review and inventory IT resources within their areas of responsibility
- **Assignment of data and or system categorization labels** — Assign categorization based on the system or data type and potential impact level
- **Approval and Review of Access Rights and Permissions** – Ensure that users, groups, and permissions are appropriate and limited to the least amount of privilege needed to perform necessary tasks
- **Risk Management** – Identification and management of risk associated with the data or asset to an acceptable level.

Data/System Custodian – An individual or group within the University that is responsible for the maintenance and operations of the technology asset/system. The asset custodian should know the asset and technical operations very well and be able to advise on the technical impact of a compromised system. The asset custodian coordinates with data owners and system owners to ensure data is properly stored, maintained, and protected. They are responsible for applying required security controls based on the categorization designated in IT0311-HSC-A-Data Security.

Data Users – the person who actually "touches" the information (enter, delete, read, process, etc.). Users are responsible for taking reasonable precautions against disclosure of data they have access to. Users should not grant access to data without proper authorizations from the Data Owner.

Campus Units – all units that collect and store data need to document their policies, procedures, and architectures that pertain to use, collection, and/or storage, regardless of the information format (electronic, paper, image, sound, etc.). This documentation should detail account creation and deletion, records retention and destruction, backup retention and destruction, and any other relevant procedures.

Standard

1. Systems/Data need to be classified in each of the areas of Confidentiality (C), Integrity (I), and Availability (A).
2. ITS has created a Qualtrics survey to enable users to answer a few questions and receive the correct categorization number. https://uthsc.co1.qualtrics.com/jfe6/preview/previewId/8202d770-f4ad-42e0-8dfb-232492165e4f/SV_0r19GDbix9pQMn4?Q_CHL=preview&Q_SurveyVersionID=current (preview)
3. The process of data and system categorization is accomplished by assigning a categorization score of 0-3 in the areas of Confidentiality, Integrity, and Availability, with higher scores representing a higher level of sensitivity or criticality. **Public information/data can have a categorization level of 0, but all other Information Technology Resources have a minimum categorization of 1.** It is acceptable if these are mixed, i.e. Confidentiality 1 (C-1), Integrity 3 (I-2), and Availability 2 (A-2).
4. Each asset will have different levels of security needs and controls based on risk, and this categorization process allows for the appropriate application of controls. This process follows the NIST recommendations in FIPS 199 by using the high watermark of the categorizations in the areas of Confidentiality, Integrity, and Availability. The highest categorization in any area will indicate if the system security plan applied is a level 1 (lowest protection level), level 2, or level 3 (highest protection level). This process and examples are illustrated in Appendix A.
5. While selecting categorization levels, System/Data Owners should also assign an impact level in the areas of Confidentiality, Integrity, and Availability to quantify the potential impact of an adverse event in each of these areas. This process, along with examples and definitions, is illustrated in Appendix A.
6. Data types should be identified and documented for each type of data that is transmitted, processed, or stored by the system or data set. These data types may

have additional statutory requirements that must be assessed regarding security control implementation in addition to the baseline controls outlined in this standard. Data types that may need to be identified and associated with a system or data set are listed in Appendix B.

7. The categorization of data is independent of its format. For example, if personal health information is revealed in a video recording of a lecture, then that video file should be classified as C-2. If paper credit card receipts are stored, then they should be classified as C-2.
8. Questions about classifying or handling the data should be directed to the Data Owner, your supervisor, or the Office of Cybersecurity. The Office of Cybersecurity can assist departmental users in developing appropriate controls and processes to protect data based on the categorization rating.
9. Report the misuse or compromise of systems that handle, store, or propagate any categorization ranking one or above IMMEDIATELY to the Office of Cybersecurity at itsecurity@uthsc.edu.

Additional considerations:

- Data is scattered everywhere; data is stored, processed, and transmitted across numerous systems, devices, and users. The categorization remains with the data and required protections follow that data.
- Context matters: the categorization and impact ratings of the system/data depends on factors such as how it used or accessed, who is using it, the volume of data, etc., and not solely on the information alone.
- The Institutional Review Board (IRB) may have additional policies or requirements regarding data associated with IRB approved studies that must be followed based on their compliance procedures.

Appendix A

Categorization, Impact, and System Security Plan Assignment

The process of data and system categorization can be accomplished by assigning a categorization score of 0-3 in the areas of Confidentiality, Integrity, and Availability. **Public information/data can have a categorization level of 0, but all other Information Technology Resources have a minimum categorization of 1.**

Confidentiality

UTHSC data and IT Resources are classified into one of four levels based on the level of concern related to confidentiality. C-3 requires the most security controls and that data should be stored in a secure enclave, and C-0 requires none.

1. Data Confidentiality Categorization: Data Owners will categorize the confidentiality of the University's Data based on the following (see paragraph II. 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.

Integrity

UTHSC data and IT Resources are classified into one of four levels based on the level of concern related to integrity. I-3 requires the most security controls, and I-0 requires none.

1. **Data Integrity Categorization:** Data Owners will categorize the **integrity** of the University's Data based on the following (see section VII for examples):

    a. 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.

    b. 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.

    c. 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.

    d. 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.

Availability

UTHSC Institutional data and IT Resources are also classified into one of four availability levels based on the level of business impact their loss of availability or service would have on UTHSC. Compromises to A-3 data or resources would cause the highest level of impact; compromises to A-0 would cause none.

1. Data that meet the following **availability** and criticality definitions criteria. Each category listed below will have different guidelines established for the business continuity and disaster recovery strategy.
    a. Business Impact Nominal (Level 0) – Data is unavailable over 2 weeks with minimal to no impact on organizational operations, organizational Assets, or individuals.
    b. Business Impact Low (Level 1) – Data is unavailable for 72 hours to 2 weeks and it could be expected to have an adverse effect on organizational operations, organizational Assets, or individuals.
    c. Business Impact High (Level 2) – Data is unavailable for 72 hours or less and it could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational Assets, or individuals.
    d. Business Impact Critical (Level 3) – Data 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 (e.g., attending athletic events).

Appendix B

Data that Must be labeled as "C-3"

"Classified" information

Data in any format that has been determined classified: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be categorized national security information; or (ii) pursuant to the Atomic energy Act of 1954, as amended, to be restricted Data (RD).

Controlled Unclassified Information (CUI)

Controlled Unclassified Information is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI is often associated with research having a DFARS or CMMC clause

Data that Must be labeled as "C-2"

Authentication information

Authentication information is data used to prove the identity of an individual, system, or service. Examples include:

- Passwords
- Shared secrets
- Cryptographic private keys
- Hash tables

Protected Health Information (PHI)

Protected Health Information is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity, and can be linked to a specific individual

Electronic Health Information (ePHI)

ePHI is defined as any protected health information (PHI) that is stored in or transmitted by electronic media. Electronic media includes computer hard drives as well as removable or transportable media, such as a magnetic tape or disk, optical disk, or digital memory card. Transmission is the movement or exchange of information in electronic form. Transmission media includes the internet, an extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media.

Payment Card Information (PCI)

Payment card information is defined as a credit card number in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

Personal Identifiable Information (PII)

PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information

Family Educational Rights and Privacy Act of 1974 (FERPA)

FERPA defines education records as any record that directly relates to a student and is maintained by an educational agency or a party acting on behalf of the institution. Examples of education records include, but are not limited to:

- Transcripts
- Degree audit reports

- Schedules of classes
- Class rolls
- Academic history reports
- Grade rolls
- Financial records

Financial Student Aid (FSA) Data
FSA data is protected by the Graham-Leach-Bliley Act (GLBA) and other security requirements outlined by the Federal Financial Institutions Examination Council (FFIEC).

General Data Protection Regulation (GDPR) Data
The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in or are citizens of the European Union (EU).

Policy History

Version #	Effective Date
1	06/16/2020
2	08/02/2020
3	12/12/2020
4	03/25/2021
5	09/09/2021
6	01/10/2022
7	01/25/2055
8	05/27/2022
9	03/001/2025 – new naming convention

References

1. NIST 800-53, Security and Privacy Controls for Information Systems and Organizations
2. NIST Glossary of Terms

3. IT0005-Data Categorization
4. IT0311-Information Technology Data Access, Management, and Recovery
5. Standards for Security Categorization of Federal Information and Information Systems (FIPS 199).
6. IT0311-HSC-D-Data Security