THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: IT0005-HSC-A Data & System Categorization	
Version 10	**Effective Date: 06/16/2020**

Responsible Office: Office of Cybersecurity	Last Review: 09/12/2025 Next Review: 09/12/2027
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 the requirements for appropriately categorizing Institutional Information and IT Resources to understand the sensitivity of data. 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 of the Institutional Information

Scope

This policy applies to all forms of data, including paper documents and digital data stored on any type of media, as well as the systems and 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

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.

Security Classification - The process of determining the security category for data or an information system.

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's 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 classification labels** – Assign classification 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 classification 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 the disclosure of data they have access to. Users should not grant access to data without proper authorization 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. ITS has created a Qualtrics survey to enable users to answer a few questions and receive the correct classification assignment. https://uthsc.co1.qualtrics.com/jfe6/preview/previewId/8202d770-f4ad-42e0-8dfb-

232492165e4f/SV_0r19GDbix9pQMn4?Q_CHL=preview&Q_SurveyVersionID=current (preview)

2. **Data Sensitivity Classification:** Data Owners will classify the sensitivity of University Data based on the following:
    a. **Public** – The effect on confidentiality of the Data is negligible. Data that would fit into this classification includes, but is not limited to:
        - Data that, by law, is available to the public without request.
        - Data on public-facing informational websites
        - Public directory information
        - Job postings
        - Published research papers
        - Press releases
        - Campus maps
        - Course information
        - Advertising
    b. **Internal Use Only** – The effect on confidentiality of the Data is minimal to minor and does not include compliance issues. Internal Use Only Data must be protected by need-to-know. Data that would fit into this classification includes, but is not limited to:
        - Routine non-public business records or reports
        - Budget information
        - Purchase requisitions
        - University insurance records
        - Routine email or internal communications not containing Private or Restricted information
        - Calendar information not containing Private or Restricted information
        - Meeting notes not containing Private or Restricted information
        - Draft or unpublished research papers using publicly available data
        - Non-public policies and procedures
        - Fundraising data
        - Opinion polls or questionnaires
    c. **Private** – Private data is classified as private due to legal, regulatory, administrative, or contractual requirements; intellectual property or

ethical considerations; strategic or proprietary value; and/or other special governance of such data. Access to, and management of, private data requires authorization and is only granted to those data users as permitted under applicable law, regulation, contract, rule, policy, and/or role. The effect on the confidentiality of Private Data is moderate. Data that would fit into this classification includes, but is not limited to:

- Trade secret or Intellectual Property protected by a non-disclosure agreement
- Tennessee Unique ID
- Employee/Faculty/Staff performance reviews
- Building floor plans showing egress routes and shelter areas
- Faculty tenure recommendations
- Data flow and IT Network infrastructure diagrams
- Security camera recordings
- Donor contact information and non-public donation amounts
- Non-public law enforcement information
- Family Educational Rights and Privacy Act (FERPA)

d. **Restricted** –Restricted data is data that requires the highest level of protection due to legal, regulatory, administrative, contractual, rule, or policy requirements. Access to, and management of, restricted data is strictly limited as unauthorized use or disclosure could substantially or materially impact the university's mission, operations, reputation, finances, or result in potential identity theft. The effect on confidentiality of Restricted Data is severe. Data that would fit into this classification includes:

- Personally Identifiable Information (PII)
- Sensitive Identifiable Human Subject Research Information (Human Subject)
- Government-issued ID numbers (Social Security Number, Driver's License Number, VISA, etc.)
- General Data Protection Regulation (GDPR)
- Personal Information Protection Law of the People's Republic of China (PIPL)
- Payment Card Industry (PCI) Data

- Financial account numbers such as banking or investment account numbers
- Protected Health Information (PHI) per the Health Insurance Portability and Accountability Act (HIPAA)
- Biometric information
- Gramm–Leach–Bliley Act (GLBA) Title IV loan Data
- Passwords, passphrases, PIN numbers, security codes, and access codes
- Controlled Unclassified Information (CUI)
- Export-Controlled Information (ITAR, EAR)

3. Any data that has not been classified by the data owner will be treated as Internal Use Only until it is properly classified.
4. 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 classification rating.
5. Report the misuse or compromise of systems that handle, store, or propagate any classification ranking one or above IMMEDIATELY to the Office of Cybersecurity at itsecurity@uthsc.edu.
6. Data Criticality Classification: See IT0311 Information Technology Data Access, Management, and Recovery for Data Criticality Classifications.

Additional considerations:

- Data is scattered everywhere; data is stored, processed, and transmitted across numerous systems, devices, and users. The classification remains with the data, and required protections follow that data.
- Context matters: the classification ratings of the system/data depend on factors such as how it is 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.

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	03/01/2025 – new naming convention
10	09/12/2025 – new naming of levels of classification

References

1. NIST Glossary of Terms
2. IT0005-Data Classification
3. IT0311-Information Technology Data Access, Management, and Recovery
4. IT0311-HSC-D-Data Security