THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: GP-005-Data Security	
Version 7	Effective Date: 06/15/2020

Responsible Office: Office of Cybersecurity	Last Review: 07/11/2023 Next Review: 07/11/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To establish security controls for data based on its sensitivity, value, and criticality to the organization. The goal is the reduction of risk to the confidentiality, integrity, and availability of UTHSC data while ensuring everyone is enabled to work.

This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This policy applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all UTHSC employees, and students, as well as to third-party agents authorized to access UTHSC data.

Definitions

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. The security categorization helps identify the appropriate level of controls to be applied to the system or data. This categorization and ranking is explained in GP–002-Data & System Classification.

Data Loss Prevention (DLP) – processes, and technology that protects against the loss of sensitive data.

Continuous monitoring – real-time visibility of users, data, and devices connected to the network.

Level 3 Data Classification – the highest of data classification level, also known as "High", these data types require the most stringent of security controls.

Maximum tolerable outage (MTO) - maximum amount of time a system or resource can remain unavailable before its loss starts to have an unacceptable impact on the goals or the survival of an organization.

Recovery point objective (RPO) - maximum targeted period in which data might be lost from an IT service due to a major incident.

Recovery time objective (RTO) - targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences.

Responsibilities

Data owner — The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division, usually a member of senior management. The data owner shall address the following:

- **Review and categorization** — Review and categorize data and information collected by their area of responsibility
- **Assignment of data classification labels** — Assign data classification based on the data's potential impact level
- **Data compilation** — Ensure that data compiled from multiple sources is classified with the most secure classification level of the highest classified data set in the compiled data
- **Data classification coordination** — Ensure that data shared between departments is consistently classified and protected
- **Data classification compliance** (in conjunction with data custodians) — Ensure that information with high and moderate impact levels is secured in accordance with federal, state, and UTHSC regulations and guidelines
- **Data access** (in conjunction with data custodians) — Develop, enforce, and follow data access guidelines for each data classification label

Data custodians — Technicians assigned responsibly for maintaining and backing up the systems, databases, and servers that store the organization's data. Data custodians are responsible for the technical deployment of all the rules set forth by

data owners and for ensuring that the rules applied within systems are working. Some specific data custodian responsibilities include:

- **Access control** — Ensure that proper access controls are implemented, monitored, and audited in accordance with the data classification labels assigned by the data owner
- **Audit reports** — Submit an annual report to the data owners that addresses the availability, integrity, and confidentiality of classified data
- **Data backups** — Perform regular backups of data based on business impact analysis, the recovery time objective (RTO), recovery point objective (RPO), and maximum tolerable outage (MTO), and backed up by UTHSC-approved solutions. Examples of non-approved solutions include Dropbox, Google Drive, and personal devices
- **Data validation** — Periodically validate data integrity
- **Data restoration** — Restore data from backup media
- **Compliance** — Fulfill the data requirements specified in the UTHSC security policies, standards, and guidelines pertaining to information security and data protection
- **Monitor activity** — Monitor and record data activity, including information on who accessed what data
- **Secure storage** — Encrypt sensitive data at rest while in storage; audit storage area network (SAN) administrator activity and review access logs regularly
- **Data classification compliance** (in conjunction with data owners) — Ensure that information with high and moderate impact levels is secured in accordance with federal or state laws and regulations as well as University guidelines
- **Data access** (in conjunction with data owners) — Develop data access guidelines for each data classification label

Data user — Person, organization, or entity that interacts with, accesses, uses, or updates data for the purpose of performing a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended and comply with this standard and all policies applicable to data use.

Chief Information Security Officer (CISO) – The person responsible for providing strategy and direction for assessment, planning, and implementation of all security standards, and practices, and ensuring compliance to same.

Chief Privacy Officer (CPO) - An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the University's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual conducts Health Insurance Portability and Accountability Act (HIPAA) risk assessments through coordination with the Information Security Agency Representative, the CISO, or the Office of Cybersecurity team, and ensures compliance with HIPAA notification and reporting requirements in the event of an identified breach.

Security/Privacy Lead - Individuals are designated by the campus/business area leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for the protection of all sensitive information under their assigned control.

Standard

1. All data and media must be protected and monitored, in a manner that reduces the risk to confidentiality, integrity, and availability while ensuring UTHSC is enabled to conduct research, work, and daily tasks consistent with UTHSC standards. Data owners review each piece of data they are responsible for and determine its overall impact level based on GP–002 Data & System Classification.
2. Data custodians and system owners coordinate with the Office of Cybersecurity to apply appropriate security controls that protect the data according to the classification label and overall impact level recorded in the official data classification table.
3. Continuous monitoring of the security, usage, and access patterns of data and systems must occur. This can be accomplished via automated solutions or manual processes that identify threats to the confidentiality, integrity, and availability of the data and systems including normal system operations, installing of updates, and ensuring changes are managed.

Reproduction of Data

When data with a level 3 classification rating is reproduced in total or in part, the reproductions shall bear the same restrictive classification as the original. Reproductions of data with a level 3 classification rating shall be kept to the minimum number of copies required to accomplish the goal. Extra care must be taken when data with a level 3 classification rating is printed and stored securely.

Storage and Security for Non-Electronic Media

All data/media with a level 3 classification rating entering or leaving work areas, processing areas, or storage facilities must be appropriately secured, such that only authorized access is permitted. Storage solutions such as filing cabinets and/or drawers used for sensitive data/media shall be secured by a lock. Data with a level 3 classification rating must be placed behind two barriers of security while being stored.

Storage and Security for Electronic Media

All data/media with a level 3 classification rating stored on electronic devices or in a digital format entering or leaving work areas, processing areas, or storage facilities must be appropriately secured, such that only authorized access is permitted. At no time shall any personal removable storage devices/BYOD, devices not issued by the University of Tennessee Health and Science Center (UTHSC) be attached to UTHSC-owned workstations with the purpose of storing and/or retrieving electronic data/media. All external storage devices shall be blocked unless it is a preapproved device issued by UTHSC. This includes cell phones, flash drives (thumb drives), external CD/DVD burners, and any other form of external storage that is not UTHSC issued. Write to CD/DVD privileges, USB drives, and external storage devices shall be removed from the ability of employees unless a business need can be proven beyond a doubt. Designated UTHSC administration, or delegated personnel, can perform unannounced inspections to confirm that all external storage devices are being stored and secured properly per guidelines. Inspections may assess whether the correct labeling and serial number for that device is provided, whether a proper log of access/chain of custody to the drive has been or is being kept, and whether the employee does indeed still have the device. The employee shall produce, on demand,

the hard drive requested for inspection by designated UTHSC staff at the exact date and time it is requested, without warning or scheduling.

Disposal/Destruction for Electronic & Non-Electronic Media

No data with a level 3 classification rating shall be disposed of by any publicly accessible means. All sensitive media must be properly disposed of in accordance with CS-001-Device Life Cycle Security.

Shipping and Manual Handling

UTHSC data/media shall not be supplied to vendors, contractors, or other external organizations without properly executed contracts, agreements, (i.e. MOU, BAA, MOA, etc.), and confidentiality agreements. Contracts and agreements shall specify conditions of use, security requirements, and return dates. UTHSC personnel involved with the movement of media shall document the movement of and the person(s) responsible for such. When shipping information with a classification rating of 3 in any area, receipt of delivery must be verified with identification and signature proof, unless otherwise action/receipt is required by law or statutory regulation.

Facsimile Transmission

The Office of Cybersecurity highly recommends that, if possible, no sensitive data be transmitted via fax. If sensitive data must be transmitted via fax the following safeguards must be followed:

- The recipient must be notified of the time it will be transmitted and agree that an authorized person will be present at the destination machine. Should an authorized person not be present, the fax machine must be in a secured area, such that unauthorized personnel may not access sent/received transmissions (i.e. fax machine is in a locked room with restricted access).
- Always use a cover sheet that includes the sender's contact information and a confidentiality statement as defined and approved by each agency's management.
- Do not include any information with a classification rating of 3 in any area on the cover sheet.
- Confirm the validity of the recipient number before sending

- UTHSC data with a classification rating of 3 in any area must not be faxed via non-trusted intermediaries like hotel staff, rented mailbox store staff, etc.
- If a fax is sent or received from an incorrect recipient, immediately notify the Office of Cybersecurity at itsecurity@uthsc.edu

**Following these precautions does not eliminate the risk of faxing. Please note that faxing over a non-secure/non-encrypted line can easily be intercepted. A fax is not recommended and should only be utilized as a last resort. **

Electronic Transmission (E-mail, File Transfer Protocol, etc.)

Data with a classification rating of 3 in any area that is sent via the internet or other media transmission facility, shall be sent securely via one of UTHSC-approved methods, i.e., encrypted email, secure file transfer protocol (SFTP), use of UT Vault. (The data owner should coordinate with the Office of Cybersecurity in determining the solution that best enables the accomplishment of their work).

Policy Exceptions

Exceptions to this Practice should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.

References

1. National Institute of Standards and Technology (NIST) 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"
2. UTSA IT Policy IT0115 – Information and Computer System Classification
3. CS-001-Device Life Cycle Security
4. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices
5. GP-002-Data & System Classification