**Policy Title:** IT6005 - Data Security Policy

**Subject Area:** Information Technology

**Responsible Official(s):** Chief Information Officer

**Responsible Office(s):** Information Technology Services

## Policy Statement

In the course of its operations, the University of Memphis collects and maintains restricted data about students, employees, donors, vendors and others. This policy governs the use, control and access to restricted data defined by statute, regulation, contract, license or definitions within this policy. The Data Classification document differentiates the types of University data.

The University of Memphis is committed to maintaining the confidentiality of all restricted University data. University data must be protected against threats such as malicious misuse, unauthorized intrusions, and/or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

Each University of Memphis department and employee is responsible for the integrity and security of University data used, controlled or accessed within their area. This policy establishes parameters for protection of University data, not the medium or application that the data resides in.

## Definitions

***Cloud-Based Service*** - A vendor-provided service including, but not limited to, storage, analytics, business intelligence, reporting, or other processing, that is not typically located within the University's physical premises.

***Data Steward*** - University officials and agents of the University who have designated duties for collection, input and maintenance responsibilities for data within their functional area.

***Encryption*** - Programs and measures to encode information such that it cannot be decoded and read without knowing an appropriate key. Transforming information using a secret key so that the information is unintelligible to unauthorized parties.

***Enterprise Information System*** - Any centralized data storage or distribution system on campus. Enterprise Information Systems are managed by ITS.

***Internal/Limited Access University Data*** - Data that would not expose the University to loss if disclosed but should also be protected. Internal/limited access University data includes, but is not limited to, operational data likely to be distributed across organizational units within the University.

***Multi-Factor Authentication*** - Multi-factor authentication (MFA) requires more than one way for people to identify themselves when logging into systems. MFA increases security.

***Network*** - Any number of computers and portable devices joined together by a physical or wireless communications link that allows information to be passed between computers, irrespective of where those computers are located. Networks provide the pathways for information traffic and allow employees to access databases and share applications residing on servers.

***Personal Identifiable Information (PII)*** - Data that can be used to uniquely identify an individual.

***Portable Devices or Media*** - Portable devices include laptops, Personal Digital Assistants (PDA), cell phones, tablets or any other portable technology hardware. Media includes technology storage mediums such as CDs, DVDs, magnetic tapes, floppy disks, external hard drives, flash drives and universal serial bus (USB) drives or any other portable storage media.

***Public University Data*** - Data available within the University community and to the general public.

***Restricted University Data*** - Data protected by federal or state law or regulations, or by contract. Restricted University data includes, but is not limited to, data that is protected by the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act (GLBA) or Controlled Unclassified Information (CUI) as identified in a law, regulation or government policy.

***Server*** - An application or hardware that performs services for connected clients as part of a client server architecture.

## Procedures

**Responsibilities**

The Chief Information Officer (CIO) is responsible for implementing appropriate data security policies, procedures and technology standards (i.e., hardware and software) for the University.

Information Technology Services (ITS) is responsible for communicating current security standards and procedures to the University community. These standards and procedures are posted on the ITS Security web page.

Department heads, in cooperation with Local Technical Support Providers called LSPs and ITS, are responsible for ensuring their employees have adequate technical support to understand and implement security standards and procedures. This responsibility extends to data regardless of the storage medium or originating point of access including, but not limited to, University-owned equipment, personally owned equipment and cloud-based services. Each unit of the University instructs employees about the designated and storage space for saved University data. In the event of an audit, each unit of the University would be responsible for providing the location of the unit's designated and approved storage.

Employees, in cooperation with their LSPs, are responsible for protecting restricted University data to which they have access. In areas not supported by a LSP, ITS will assist employees. Employees are required to complete the annual ITS security awareness training.

Employees are responsible for ensuring that appropriate security controls, in accordance with published University standards, are in place to protect restricted University data. This responsibility extends to data regardless of storage media or originating point of access including, but not limited to, University-owned equipment, personally owned equipment and cloud-based services.

Employees are responsible for maintaining a clean desk and clear screen and for protecting university data regardless of the medium on which it resides, including paper. Employees shall secure sensitive data by adopting principles related to clean desks and clear screens to diminish the likelihood of data loss and unauthorized access to data. When necessary, screens shall be located in a manner to prevent bystanders from inappropriately viewing. Media containing restricted data must be securely stored or destroyed, including shredding paper copies when appropriate.

Personal passwords are established and secured by account holders. In accordance with IT6003 - Acceptable Use of Information Technology Resources policy, passwords are not to be disclosed or shared. Multi-factor authentication is required for all account holders prior to accessing University computer resources unless an exception is granted by the CIO.

The ITS Security web page should be reviewed at the beginning of each academic semester by all account holders.

**General Security**

In coordination with the Office of Legal Counsel and the Department of Internal Audit, ITS will develop appropriate specific procedures for compliance with this policy and provide education

to the University community on the implementation of this policy and such procedures. Procedures, technology standards and best practices can be found at the ITS Security web page.

University data must be saved to an appropriate location defined by the Guidelines for Data Storage based on the data classification except for rare exceptions approved by the Information Security Advisory Committee (ISAC). Data stewards may request to store unencrypted restricted data through the CIO's office, and the request will be forwarded to ISAC for approval. The request acceptance or denial will be noted in the minutes of the ISAC meeting following the request.

If ISAC grants permission for University data to be saved and stored on University-owned equipment, personal equipment or cloud-based services, faculty and staff are personally responsible for encrypting the data with the current ITS standards and for remembering the encryption keys or passwords. Access to saved and stored University data while on campus must be through the University's network.

Restricted University data must be protected against physical theft or loss, electronic invasion or unintentional exposure through a variety of personal and technical means.

Prior to use of restricted University data via laptop computer or other portable storage media, employees are responsible for obtaining appropriate protections for such computers or portable devices, or for verifying that such protections are already in place. The use of unprotected equipment to access or store University data is prohibited, whether or not the equipment is owned or controlled by the University, unless an exception has been granted by the CIO.

All University computers must have recommended operating system patches and updates installed, updated firmware, updated antivirus and antispyware tools installed, and firewalls turned on. Other devices connected to the University's network must utilize appropriate security protections to the extent possible, including updated firmware.

ITS is responsible for the security of all Enterprise Information Systems throughout campus, including but not limited to, enterprise resource planning and associated systems such as Banner, Active Directory and the UMmail e-mail system.

ITS will audit servers, computers and portable devices or media for compliance with policies and standards and will deny network access for servers, computers and portable devices or media out of compliance with current best practices.

**Remote Access**

Remote access to restricted University data is available only to authorized employees. Employees must be authenticated to access restricted University data remotely. Data must be encrypted during transit.

Remote access to University systems is available using approved methods. All remote access to the University's network and computer systems is required to use one of the secure methods outlined in the section of Remote Access to University Network section of the ITS Security Best Practices web page.

**Personal Computers**

Personal computers that are used to access, store or transmit restricted University data should use current security patches, encryption and updated antivirus and antispyware software. In instances where standard security precautions are not free, the employee will incur all costs for security of their personal computer.

Employees are responsible for deleting all restricted University data from their personal computer upon termination of employment or change in employment when access to the data is no longer required to complete job duties.

**Portable Devices, Media and Cloud-Based Services**

Each user in the possession of restricted University data is responsible for protecting the data, regardless of the media or location where the data resides.

Restricted University data may not be stored on any portable device, media or cloud-based service unless protective measures are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss. Protective measures must be implemented before restricted University data is stored on portable devices, media or cloud-based service.

Restricted University data stored on portable devices or media must be encrypted with the University's data encryption standard. Cloud-based services shall include encryption protection through appropriate business agreements.

**Equipment Disposal**

University-owned computers, portable devices and media must have University data securely erased prior to its transfer out of University control, and/or destroyed, using current best practices. Lost or stolen equipment storing restricted University data must be reported as a Security Incident.

**Failure to Comply with this Policy**

Failure to comply with this policy may result in limiting or denying access to University data resources. If, upon investigation by the appropriate University officials, the lack of compliance appears to have been willful and deliberate or if there is repeated lack of compliance, disciplinary action may be taken, up to and including termination.

The ITS Security web page should be reviewed at the beginning of each academic semester by all users.

## Related Documents, Policies and Forms

Data Classification Document
Data Storage Guidelines
Family Educational Rights and Privacy Act (FERPA)
Health Insurance Portability and Accountability Act (HIPAA)
Gramm-Leach Bliley Act (GLBA)
Controlled Unclassified Information (CUI)
State of Tennessee Data Security Law
IT6003 - Acceptable Use of Information Technology Resources
IT6004 - Security and Protection of Electronic Information Resources
IT6000 - Data Access
TigerLAN Guidelines
ITS Security Procedures and Best Practices
BF4013 - Red Flag Policy

## Last Revision Update Log: 03/02/2023

IT6005 – revised April 7, 2021
IT6005 – revised March 14, 2019
IT6005 – revised March 27, 2018—supersedes
UM1691 – revised October 7, 2016
UM1691 – revised October 9, 2014
UM1691 – revised April 26, 2014
UM1691 – revised April 17, 2013
UM1691 – revised November 10, 2009
UM1691 – issued November 5, 2008 - supersedes policy number 1:2A:03:05