Policy 01:004 – Data Storage

1. Purpose

The University of Montevallo ("University") is responsible for ensuring security and access to University data. This policy establishes guidelines for the storage of University data to ensure its integrity, confidentiality, and availability in compliance with applicable federal and state laws and regulations and other University policies.

2. Scope

This policy applies to all University faculty, staff, students, official University affiliates, or any other individual, group, or office with University-approved access to data owned, leased, or used by the University (hereafter, the "User" or "Users").

3. Policy Statement

All University data is grouped into three classifications; Restricted, Confidential, and Public (See 01:009 – Data Governance for further details). Information Services & Technology (IS&T) offers Users a variety of secure file storage options for retaining University data. This policy provides general guidelines on the appropriate storage options and procedures as determined by data classification. Additionally, the University's Data Governance Committee (DGC) annually reviews data governance procedures and practices, including those associated with secure data storage, and provides updated storage guidelines to all relevant campus Units.

3.1. Data Storage:

Stand-Alone Computer: To safely store University data on or with a University-owned Stand-Alone Computer, Users are responsible for ensuring the physical security and appropriate use of the Computer(s) assigned to them or under their authority. The following guidelines and conditions describe the responsibility of the User in protecting University data when using a Stand-Alone Computer.

- Stand-Alone Computers will be in physically secure areas which can be locked when not in use
- Access to Stand-Alone Computers will be limited to individuals engaged in official University business
- Use of Stand-Alone Computers by student workers should be restricted to those cases in which student workers are necessary to supplement regular University staff members. Student workers should be thoroughly instructed in the proper and responsible use of computers and information security

- Individuals with access to administrative information are assigned personal account credentials (user id and password) and are not to share this information with anyone else
- Under no circumstances will account credentials be posted on or near computers
- Stand-Alone Computers on which an individual has "signed on" should never be left unattended
- Restricted or Confidential data must only be stored temporarily on Stand-Alone Computers and portable storage devices
- Because of the possibility of theft and discovery of data, neither portable computers (notebooks, laptops, etc.) nor portable storage devices, including USB drives, shall be used to store data classified as Restricted or Confidential, unless such data is encrypted.

3.2. ***Cloud-Based Storage:*** University-Approved Cloud-Based Storage, not the computer's hard drive, is the preferred storage method for Stand-Alone Computer Users. To meet current data security requirements, the following conditions or restrictions shall be placed on collecting, processing, storing, or sharing certain data within the cloud environment.

- All Users must only use University-approved cloud-based storage platforms for Restricted or Confidential data.
- Restricted or Confidential data are not permitted to synchronize with non-University owned devices or storage.
- Sharing Restricted or Confidential data outside the University must be approved by the appropriate Data Trustee or Data Steward.
- Cloud-based file storage services not approved by the University shall not be used to store Restricted or Confidential University data. Users who do so will assume responsibility and be held personally liable for any data breach or policy or legal violation that results from utilizing a cloud-based file storage provider not approved by the University.

3.3. ***On-Site Storage Area Network:*** An On-Site Storage Area Network (SAN) managed by IS&T is the preferred storage method for most Restricted or Confidential data. All On-Site SANs are protected by intrusion detection systems and routine security audits.

3.4. ***Remote Access:*** While University- and non-University owned computers and Mobile Devices may be used to access University data remotely, access must be through a University-approved Virtual Private Network (VPN).

3.5. ***File Storage Options:*** The following table provides general guidelines on data storage based on classification. IS&T is available for questions or consultation on appropriate data storage options.

	Restricted	Confidential	Public
On-Site Storage Area Network (SAN)	Yes	Yes	Yes
UM-Approved Cloud-Based Storage (e.g., OneDrive or Box)	Yes	Yes	Yes
Stand-Alone Computer (Desktop or Laptop)	Temporarily	Temporarily	Yes
Non-UM-Approved Cloud-Based Storage	No	No	Yes
Non-UM-Owned Stand-Alone Computer or device	No	No	Yes
Mobile Device	Temporarily	Temporarily	Yes
Remote Device	Temporarily	Temporarily	Yes
Portable Storage Device	No	No	Yes

4. Definitions

Cloud-Based Storage: A mode of data storage in which digital data is stored on servers in off-site locations. The servers are, typically, maintained by a third-party provider who is responsible for hosting, managing, and securing data stored on its infrastructure.

Mobile Device: A University- or non-University-owned device, such as a smartphone or tablet, used to access university data or information from any on- or off-campus location. Please see Policy 01-024 – Mobile and Remote Devices for further information.

On-Site Storage Area Network (SAN): A network of storage devices that can be accessed by multiple servers, systems, or computers, providing a shared pool of storage space.

Portable Storage Device: A device that can be externally connected to a computer or network to provide data storage. Examples: USB flash drive or external hard drive.

Remote Device: A University- or non-University-owned device, such as a laptop or desktop computer, used to access university data or information from any off-campus location. Please see Policy 01-024 – Mobile and Remote Devices for further information.

Stand Alone Computer: Any University-owned desktop or laptop assigned to an individual or department. Generally considered a personal computer for faculty and staff provided by the University but, in some cases, may also be a computer shared by multiple members of a department or a computer available for check out by University employees.

Temporarily: In reference to data storage, temporary storage means that data files may be downloaded when immediate access is needed or required but are not to remain on the device for future access.

5. Policy Approval, Review, and Administration

Responsible Office(s): Information Services & Technology

Responsible Individual: Chief Information Officer

Effective Date: 08/2024

Last Revision: None