Policy 01:024 – Mobile & Remote Devices

1. Purpose

Mobile and Remote Devices are important tools at the University of Montevallo ("University"), and their use is supported to advance the mission of the University. Mobile & Remote Devices also represent a significant risk to information and data security. Appropriate security measures and procedures are required to prevent these devices from serving as conduits for unauthorized access to University data and IS&T resources. This policy is to promote and ensure data and information security by establishing requirements for Mobile & Remote Device use.

2. Scope

This policy applies to all University of Montevallo ("University") faculty, staff, students, official University affiliates, or any other individual, group, or office that uses personal or university-owned Mobile or Remote Devices to access any non-public University data or technology resources (hereafter, "User" or "Users").

3. Policy Statement

Mobile and Remote Device Users are responsible for any institutional data that is stored, processed, and/or transmitted via that device and for following all security requirements set forth in this policy.

Mobile Device Security Measures: All users of a Mobile Device used to access non-public University systems must take the following measures to secure the device when on campus. (1) Register the device via the appropriate Wi-Fi registration process if the device will access any non-public University network system. (2) Configure the device to automatically lock after being idle and require a password to regain access.

Remote Device Security Measures: While personal, 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).

Storage of Confidential and Restricted Data: In general, Confidential and Restricted Data should not be stored on Mobile or Remote Devices. However, in certain instances and depending on job responsibilities, this may be unavoidable. In these instances, confidential data must be stored on University-owned devices only with the following requirements:

- Except when being actively used, Confidential and Restricted Data must always be encrypted on any device through a mechanism approved by the

University. Alternatively, whole drive encryption software may be deployed to meet this requirement.

- Mobile devices must have University-supported software enabled and running to identify, protect, and respond to any threats to the data or operating systems of the devices.
- University-owned Mobile Devices must have Mobile Device Management software installed to facilitate device protection, including remote wipe and, if possible, device location technology for recovery.

Violations of policy or law may result in University sanctions, disciplinary action including immediate termination of employment, expulsion as a student, and/or other legal action.

4. Definitions

Mobile Device: Includes telecommunication and portable computing devices which can execute programs or store data, including but not limited to tablet computers and smartphones. Generally, a device capable of using the services provided by a public/private cellular, wireless, or satellite network.

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.

5. Policy Approval, Review, and Administration

Responsible Office(s):	Information Services & Technology
Responsible Individual:	Chief Information Officer
Effective Date:	08/2024
Last Revision:	None