Auburn University at Montgomery
Policies and Procedures

Title: Mobile Device Encryption Policy

Responsible Office: Office of Technology

I. PURPOSE

The purpose of this policy is to establish the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption.

II. POLICY

The large volume of electronic data stored on computer systems and electronic media throughout the University includes confidential and sensitive information, such as student records, financial data, personnel records and research information. The University is subject to: federal laws that set forth responsibilities for protecting this information, copyright laws, and software license agreements that protect vendor rights regarding the use of software.

Theft or loss of mobile devices may result in unauthorized disclosure of sensitive information. Such Disclosure may subject the University to legal liability, negative publicity, monetary penalties and loss of funding. Therefore, encryption is required for all laptops, mobile workstations, and portable drives that may be used to store or access confidential and sensitive data.

This policy outlines the responsibilities for carrying these protective measures.

III. EFFECTIVE DATE

December 1, 2017

IV. APPLICABILITY

This policy applies to all departments, faculty, employees, students and contracted personnel that use or maintain AUM information systems or media which contains sensitive or confidential information.

V. RESPONSIBILITY

The primary responsibility for the protection of data that resides on laptops, mobile workstations systems, or and portable drives rests with the units that procured, purchased, or leased and/or manages the device.

Policy Responsible Office: Office of Technology
Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

Mobile workstation refers to computer systems such as desktop computers that have a multi-use such as university events and/or are moved to different locations.

Portable Drive refers to an external storage device that plugs into a USB, FireWire, or eSATA port on a computer and is used for backup, secondary storage, or transport of data.

Confidential and sensitive information include, but are not limited to, Social Security Numbers, student educational records, health care records, bank account and other financial information, research data, personnel data, other confidential or sensitive University business information, or any Personal Identification Information (PII) data not listed here.

VII. PROCEDURES

Devices and Media

Encryption is required for all laptops and portable workstations that may be used to store or access AUM data. Encryption is required for all portable drives that are used to store confidential and sensitive information. ITS will provide, install, configure, and support encryption where it is needed. It is the responsibility of the department to notify ITS if any devices or media need to be encrypted.

Electronic Data Transfer

Electronic Data Transfer of confidential and sensitive information must take place utilizing encryption. Encrypted data may be transmitted via encrypted or unencrypted channels. All email communications that involve email addresses outside of AUM use an unencrypted channel, and therefore require that messages containing confidential and sensitive information be encrypted. Approved methods of encrypting electronic data transfers include but are not limited to Transport Layer Security (TLS1.1 or TLS 1.2), Secure Socket Layer (SSL) Protocol, SSH File Transport Protocol (SFTP), or ITS-approved Virtual Private Network (VPN) connection. If the encryption method includes a password, that password must be transferred through an alternative method, such as calling the individual. Email messages containing encrypted data may never include the password in the same message as the encrypted data.

Physical Transfer of Electronic Data

Any time AUM confidential and sensitive information is placed on a medium such as a CD, DVD, or portable drive to facilitate a physical transfer, either entirely within AUM or between AUM and a 3rd party, that data must be encrypted. Archiving or backing up confidential and sensitive information to a physical medium is permitted if the data or the physical medium is encrypted.

Encryption Standards

Only whole disk encryption solutions approved by the Office of Technology may be utilized to satisfy the requirements of this policy. The entire disk, or all user-writable local disk volumes, will be encrypted by ITS. ITS will centrally maintain copies of encryption keys and encryption audit logs. ITS retains the right to decrypt data using the centrally maintained key as required.

VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy will be considered a Group I infraction under the University Personnel Manual and is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

NONE

X. INTERPRETATION

The Office of Technology CIO has the authority to interpret this policy.

APPROVAL TO PROCEED: _____ **DATE:** 12-1-17

APPENDICES

NONE