Data Encryption Policy

I. POLICY STATEMENT

All mobile computing devices used by University employees must be encrypted.

Auburn University **confidential data** stored on any computing device or storage media must be encrypted unless stored in a secure location approved by the Information Security Office.

Auburn University **operational data** stored on any computing device or storage media should be encrypted.

II. POLICY PRINCIPLES

All computing and storage devices that access, store, process or transmit **University Data, regardless of ownership,** must be compliant with Auburn University Information Security Policies and Standards.

III. EFFECTIVE DATE

Adopted: October 1, 2015
Revised: June 14, 2018

IV. APPLICABILITY

This policy applies to all Auburn University employees.

V. POLICY MANAGEMENT

***Responsible Office*:** Office of the CIO

***Responsible Executive*:** Chief Information Officer

***Responsible Officer*:** Chief Information Security Officer

VI. DEFINITIONS

Mobile Computing Device: laptop or notebook computers, tablet computers, smart phones, and other easily portable devices used to access, view, or modify University Information.

Mobile Storage Device: thumb drives, USB drives, SD (or similar) memory cards, USB-attached hard drives, and other easily portable devices used to store University Information.

University Information: Data that Auburn University or an Auburn University employee creates, receives, maintains, manages, transmits or stores as a result of or in support of any administrative, educational, clinical, research or patient care/clinical activities and any such data for which Auburn University is responsible by law, policy or contract.

VII. POLICY PROCEDURES

All devices requiring encryption must meet the following criteria:

1. The encryption passphrase will meet or exceed Auburn University password strength requirements, must not be shared, and not stored in a visible or plaintext form on or with the device.

2. Devices where keyboard entry is cumbersome (ex. Smartphones) may use reduced password complexity if the device is configured to allow no more than 10 failed password entry attempts before preventing use by locking for a significant amount of time or erasing all storage.

3. Whenever possible, the encryption system will include a management component that provides for key recovery and proof that the device is encrypted. When this is not possible, an alternative method must be provided to satisfy the key recovery and proof of encryption requirements.

4. Whenever possible, devices will include the ability to remotely wipe stored data in the event the device is lost or stolen.

5. The computing device must be configured with an inactivity timeout of not more than 15 minutes, which requires re-authentication before use. Shorter timeout durations should be implemented when appropriate based on risk and usage.

The encryption and key management methods used must have the approval of the Auburn University Chief Information Officer or designee.

VIII. SANCTIONS

Deliberate violation 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

1. Specific uses where no Confidential or Operational Data will be stored and encryption would interfere with the device's intended use: devices used in this way must be clearly marked as not for use with Confidential or Operational Data.

2. Specific uses in which devices are used for marketing and public relations, and no Confidential or Operational Data will be stored: devices used in this way must be clearly marked as not for use with Confidential or Operational Data.

X. INTERPRETATION

Office of the Chief Information Officer