Mobile Device Encryption Policy

Responsible Office: **Office of the Chief Information Officer**

I. POLICY STATEMENT

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

II. POLICY PRINCIPLES

All mobile 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

October 1, 2015

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*:** University Information Security Officer

VI. DEFINITIONS

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

Portable 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.

Restricted Information: Data that falls into the category of “Confidential” or “Operational” as defined in the University Data Classification Policy.

VII. POLICY PROCEDURES

All portable computing devices, laptops, phones, tablets belonging to the University must be encrypted.

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. Small portable computing 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 portable computing device must be configured with an inactivity timeout of not more than 30 minutes, which requires re-authentication before use. Shorter timeout durations should be implemented when appropriate based on risk and usage.

All portable storage devices must be fully encrypted. The following exceptions apply:

1. Specific uses where no Restricted 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 Restricted Data.

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

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

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

1. Specific uses where no Restricted 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 Restricted Data.

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

X. INTERPRETATION

Office of the Chief Information Officer