# Information Security Policy

## I. POLICY STATEMENT

All entities at Auburn University are responsible for the security of information within their control.

## II. POLICY PRINCIPLES

Auburn University has in its possession, for the express purpose of supporting the University's mission, large quantities of computerized information relating to faculty, staff, students, researchers and vendors. Some of this information is private and confidential, as defined by the Data Classification Policy.
It is the responsibility of each individual with access to information resources to use these resources in an appropriate manner and to comply with all applicable federal, state, and local statutes and Auburn University policies. Additionally, it is the responsibility of each individual with access to confidential or operational data resources to safeguard these resources.

## III. EFFECTIVE DATE

Adopted: May 4, 2005
Revised: May 31, 2017

## IV. APPLICABILITY

This policy applies to all Auburn University employees, students, and agents.

## V. POLICY MANAGEMENT

OIT and College/School/Department leadership is responsible for the management of computers and information within their control.

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

## VI. DEFINITIONS

None

## VII. POLICY PROCEDURES

Methods of safeguarding sensitive data include:

1. Confidential data should not be stored on desktop, laptop, or tablet computers; mobile computing devices; or media storage devices unless encrypted since these type devices tend to reside in less secure locations.

2. Access to computers that are logged into systems storing confidential or operational data should be restricted (e.g., authenticated logins and screen savers, locked offices, etc.)

3. Access to confidential and operational data should be restricted to those individuals with an official need to access the data.

4. All servers containing confidential data must be housed in a secure location and operated only by authorized personnel and must be registered with Office of Information Technology using the Auburn University System Registry (AUSR)

5. Copies of confidential and operational data should be limited to the fewest practical locations.

6. Confidential data must be transmitted in a secure encrypted manner.
7. Servers/systems which meet the Confidential Data/Server Security Standards may host confidential information upon approval by the Office of the CIO.
8. Any accidental disclosure or suspected misuse of confidential data should be reported immediately to the Chief Information Security Officer, abuse@auburn.edu, or 844-0888.
9. Users will be authenticated to all Auburn University systems. Multiple authentication mechanisms may be used including but not limited to single level passwords or 2-factor authentication.
10. Passwords must meet Auburn University's minimum password standards. At a minimum passwords will be 8 characters in length, and must have at least three of the following criteria: 1) contains an upper case letter, 2) a lower case letter, 3) a number or 4) a special character.
11. All remote access to confidential and operational data on the Auburn Network will require 2-factor authentication. In addition, the Office of the CIO may mandate where 2-factor authentication will be required.
12. At a minimum passwords will be changed every six months.

## VIII. SANCTIONS

Deliberate violation of this policy will be considered a Group I infraction under the Auburn University Personnel Policies and Procedures Manual and is subject to disciplinary action, up to and including dismissal.

## IX. EXCLUSIONS

None.

## X. INTERPRETATION

The Auburn University Chief Information Officer has the authority to interpret this policy.

# APPENDICES

*Attach a full version, in PDF format, of the submitted policy and supporting documents (i.e. forms, exhibits, memorandums etc.)*