# 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 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
Revised: May 15, 2019

## IV. APPLICABILITY

This policy applies to all Auburn University employees, students, and others granted access to Auburn Information.

## 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.

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. Web Applications with access to confidential or operational data must use the University approved single sign-on (SSO).

11. Applications that use simple LDAP binds or other non-secure methods of authentication to Auburn's Active Directory LDAP are prohibited.

12. Caching or storing of clear-text passwords is forbidden.

13. The use of email protocols that do not support two factor authentication will only be allowed when connected to the on-campus network.

14. User passwords must meet Auburn University's minimum password standards. New passwords must be between 12 and 32 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.

15. Privileged domain accounts (domain admin, enterprise admin, AD, LDAP, RADIUS/VPN, NetWare) require a minimum of a 20-character password 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.

16. Users should not reuse their passwords. When practical, password history will be set to remember the last 10 passwords to reduce password reuse.

17. All remote access to confidential and operational data on the Auburn Network will require 2-factor authentication.

18. All remote access to the Auburn network will require the use of OIT approved two factor authentication; this includes but is not limited to VPNs, Remote Desktop Programs, Secure Shell (SSH) and Virtual Desktop Infrastructure access.

19. Whenever practical, access to data defined in the Sensitive Personally Identifying Information Protection Policy (i.e. SSN, Driver's license Number, Passport numbers, bank

routing numbers, etc.) should implement 2-factor authentication. In addition, the Office of the CIO may mandate additional areas requiring 2-factor authentication.

20. At a minimum, passwords will be changed every twelve months. Passwords not changed after 12 months will be forced to be changed on the next login.
21. All computers (i.e. student, employee, agents) connected to the Auburn University Network or storing Auburn University confidential or operational data must be protected by current anti-virus software.
22. Users should lock their screen or logoff when leaving their devices. Desktops, laptops, and other personal devices will have an inactivity timeout of no more than 15 minutes.

## 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.