Information Disclosure and Confidentiality Policy

I. POLICY STATEMENT

Individuals with access to Auburn University confidential information or data bear the responsibility to respect and maintain the privacy and security of confidential information and data. Individuals must comply with all applicable University and departmental policies, state and federal laws governing privacy of information.

II. POLICY PRINCIPLES

Individuals must understand their responsibility to protect and safeguard confidential information and data to which they have access because of their affiliation with Auburn University.

a) Individuals must hold all confidential information and data in trust and confidence, and will only use, access, store, or disclose confidential information or data, directly or indirectly, as appropriate in the performance of the their assigned role or duties for Auburn University.

b) Individuals must comply with all applicable state and federal laws and University policies relating to the access, use, and disclosure of confidential information and data.

c) Individuals shall not remove material or property containing confidential information or data from their department or program area unless it is necessary in the performance of the person's assigned duties or role. If materials or property containing confidential information or data must be removed from the department or program area, the individual must safeguard the materials/property in accordance with the *Data Classification Policy* and related guidance.

d) Individuals will not seek to obtain or access any confidential information or data involving any matter, which does not involve or relate to the person's job duties or role.

e) Access to confidential data as part of an individual's assigned responsibilities or role does not necessarily constitute authority to release such information to other employees, parents, students, or third parties. In all circumstances, any disclosure must be in accordance with all applicable laws and University policies.

f) If an individual has any question relating to the appropriate use or disclosure of confidential information or data, the individual shall consult with their data steward, supervisor or other appropriate University personnel.

g) Upon termination or expiration of employment, contracted responsibilities, volunteer activities, or other University-affiliated role, individuals shall have access to confidential information or data removed. Additionally, any documents, reports, or correspondence containing confidential information or data must be returned to their supervisor or other designated University representative.

h) Individuals must promptly report to their supervisor or designated University representative any known or suspected violations of this policy

III. EFFECTIVE DATE

October 1, 2017

IV. APPLICABILITY

This policy applies to all individuals with access to University data.

V. POLICY MANAGEMENT

Responsible Office: Division of Institutional Compliance & Privacy
Responsible Executive: Associate VP Audit, Compliance & Privacy
Responsible Officer: Director, Institutional Compliance & Privacy

VI. DEFINITIONS

Confidential information or data: Information that is required to be strictly protected. There are often governing statutes, regulations or standards with specific provisions that dictate how this type of data must be protected. For more information, see the University *Data Classification Policy* and related guidance.

VII. POLICY PROCEDURES

N/A

VIII. SANCTIONS

Deliberate disregard of this policy or principles may result in discipline up to and including dismissal. Some violations may constitute criminal or civil offenses.

IX. EXCLUSIONS

None.

X. INTERPRETATION

This policy is subject to interpretation by the Division of Institutional Compliance & Privacy