Data Classification Policy

I. POLICY STATEMENT

Auburn University ("the University," "University") data will be classified into categories by its sensitivity and criticality. Data will be handled in accordance with the *protections standards* promulgated by the Office of the Chief Information Officer.

II. POLICY PRINCIPLES

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with the value, sensitivity, and criticality of the data, allowing the University to implement security at the appropriate level, to establish guidelines for legal/regulatory compliance, and to reduce or eliminate conflicting standards and controls.

III. EFFECTIVE DATE

January 1, 2015

IV. APPLICABILITY

This policy applies to all University colleges, departments, administrative units, and affiliated organizations. For the purposes of this policy, "affiliated organization" refers to any organization associated with the University that uses university information technology resources to create, access, store, or manage University data. It also applies to any third party creating, storing, or maintaining University Data per a contractual agreement.

V. POLICY MANAGEMENT

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

VI. DEFINITIONS

Data: Items of information that are collected, maintained, and used for the operations of the University, regardless of the storage medium or access method.

Confidential data: Confidential data is business or personal 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. Access to confidential data is limited to persons with authority to view or use the data and may not be shared with or disclosed to persons without such authority; it may be used only for those purposes that are a part of the user's university responsibility. Unauthorized disclosure of this information could have a serious adverse impact on the University, individuals or affiliates.

Regulations, laws and standards that affect data in this category include, but are not limited to, the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.), the Export Administration Regulations (15 CFR 730 et seq.), the Health Insurance Portability & Accountability Act (HIPAA) and Payment Card Industry (PCI) standards, Family Educational Rights & Privacy Act (FERPA) and the Graham-Leach-Bliley Act (GLBA).

Examples:

Biometric data, Credit Card Information, Passport Numbers, State Issued Driver/Non-Driver License Numbers, Military Identification, Bank Account Number, Health Insurance Policy Number or subscriber

information number, Export Controlled Data, Protected Health Information (HIPAA), Medical History Information, Social Security Numbers (SSNs), Information involving National Security. Student data that is not designated directory information; certain research (e.g. proprietary or otherwise protected).

Operational data: Operational data includes information that is not openly shared with the general public but is not specifically required to be protected by statute, regulation or by department, division or University policy. It is intended for use by a designated workgroup, department or group of individuals within the University. Unauthorized disclosure of this information could adversely affect the University, individuals or affiliates.

Note: While some forms of sensitive data can be made available to the public, it is not freely disseminated without appropriate authorization.

Examples:

Personally identifiable information (PII) such as name, birthdate, address, employee/student ID, etc. when held in combination in a way that could lead to identify theft or other misuse, budget information, personal phone numbers, employment applicant information, departmental policies and procedures, internal emails, documents or memos, incomplete or unpublished research, human resource information.

Public data: Public data is purposefully made available to the public by some valid authority and may be freely disseminated without potential harm to the University or its affiliates.

Examples:

Advertising, product and service information, directory listings, published research, presentations or papers, job postings, press releases, instructions, training manuals.

VII. POLICY PROCEDURES

The University Security Information Office issue maintain protection standards and policies for the handling of the various data classification categories.

The Information Security Office will maintain data storage matrix to guide users in storing confidential, operational, or public data.

Consult with an IT provider or contact the Information Security Office by sending a request to infosec@auburn.edu to determine the proper standards.

VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

There are no exclusions to this policy.

X. INTERPRETATION

For interpretations of this policy please refer to the Chief Information Security Officer.

Adopted: December 18, 2014
Revised: May 17, 2018