SOUTHERN UNIVERSITY AND A&M COLLEGE SYSTEM
**Division of Information Technology**

# DATA CLASSIFICATION POLICY

## Purpose:

This document provides a framework for securing data from risks including but not limited to, unauthorized destruction, modification, disclosure, access, inappropriate use and removal. This policy outlines measures and responsibilities required for securing data resources. It shall be carried out in conformity with state and federal law.

This policy serves as a foundation for the University's information security policies, and is consistent with the University's data management and records management standards. It is not the purpose of this policy to create unnecessary restrictions to data access or use for those individuals who use the data in support of University business or academic pursuits.

## Scope:

This policy applies to all university administrative data and to all user-developed data sets and systems that may access these data, regardless of the environment where the data reside (including cloud systems, servers, personal computers, mobile devices, etc.). The policy applies regardless of the media on which data resides (including electronic, microfiche, printouts, CD, etc.) or the form they may take (text, graphics, video, voice, etc.). This applies to all university systems in each college, school or department regardless of geographic location. Systems impacted by a natural disaster are not included in the scope of this document.

This Policy applies to all faculty, staff and third-party agents of the University as well as any other University affiliate who is authorized to access institutional data. In particular, this policy applies to those who are responsible for classifying and protecting institutional data.

## Policy:

As part of the information security program, information assets must be identified, classified, tracked and assigned guardianship to ensure that they are protected against unauthorized exposure, tampering, loss, or destruction and that they are managed in a manner consistent with applicable federal and state law, the University's contractual obligations, their significance to the University, and their importance to any individual whose information is collected. In order to achieve this objective, information must be classified to convey the level of protection expected by all employees or agents who are authorized to access the information.

1. Information Asset Collections. For purposes of managing information, the University's various types of information must be segregated into logical collections, e.g. student records, financial records, employee benefit data, payroll data, medical records, personal information regarding alumni, etc. The security requirements for each collection are defined by the information's needs for confidentiality, integrity and availability.

2. Information Asset Classification. To implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data, data will be classified into one of the following categories. By default, all institutional data that is not explicitly classified should be treated as confidential data.

    1. *Restricted.* Data is classified as restricted when there are legal, contractual or regulatory requirements regarding the storage and disclosure of the data. Unauthorized disclosure or modification of Restricted data would necessitate notifying federal or state authorities and/or the affected individuals. Examples of Restricted data include Personal Health Information, Personally Identifiable Information (Social Security Numbers), financial account or payment card information, authentication or authorization information to electronic resources.

    2. *Confidential.* Data is classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. This information can be shared only on a "need to know" basis with individuals who have been authorized by the appropriate Data Trustee, Data Steward or designee, either by job function or by name. The disclosure of confidential data to unauthorized persons may be a violation of federal or state laws or University contracts. Examples of Confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to confidential data.

    3. *Internal.* Data which the Data Trustee or Stewards may choose to publish or make public and data protected by contractual obligations. Sharing such information with individuals outside the University community requires authorization by the appropriate Data Trustee, Data Steward or designee.

    4. *Public.* This information can be freely shared with individuals on or off-campus in accordance with state and federal regulations without any further authorization by the appropriate Data Trustee, Data Steward or designee. Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the University and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are

required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

3. Data in all categories will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business or research functions of the University, result in financial loss, or violate law, policy or University contracts.

4. Information integrity and availability. For purposes of integrity and availability, information systems will be classified as follows:

   1. Non-Critical Systems. Information systems fall into this category if the unavailability, unauthorized modification, loss or destruction of the data residing on the system would cause little more than temporary inconvenience to the staff and user community and incur limited recovery costs. Reasonable measures to protect information deemed non-critical include storing information in locked office spaces or cabinets, using standard access control mechanisms to prevent unauthorized individuals from altering digital information, and making regular backup copies.

   2. Critical Systems. Information systems fall in this category if unavailability, unauthorized access/modification, loss or destruction through accident, malicious activity or irresponsible management could potentially cause the University to 1) be unable to conduct a portion of its required business for an extended period, 2) suffer significant damage to its reputation, 3) endure major financial loss, 4) fall out of compliance with legal, regulatory or contractual requirements, or 5) adversely impact members of the extended University community.

      1. Additional Safeguards

         1. Data Elements in systems should be sampled and checked for validity on a regular basis.

         2. A business continuity plan to recover critical information that has been lost must be developed, documented, deployed and tested annually.

      2. Security. Security measures for data are set by the data custodian, working in cooperation with the data stewards.

      3. Responsibilities. The following roles and responsibilities are established for carrying out this policy:

         1. Data Trustee: Data trustees are senior University officials (or their designees) who have planning and policy-level responsibility for data within their functional areas

and management responsibilities for defined segments of institutional data. Responsibilities include assigning data stewards, participating in establishing policies, and promoting data resource management for the good of the entire University.

    2. Data Steward: Data stewards are University officials having direct operational-level responsibility for information management - usually department directors. Data stewards are responsible for data access and policy implementation issues. Procedures for performing data validation should be developed and implemented by data stewards in responsible departments

    3. Data Custodian: Information Technology (IT) is the data custodian. The custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by data trustees or their designees (usually the data stewards), and implementing and administering controls over the information.

    4. Data User: Data users are individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to non-public data have a position of special trust and as such are responsible for protecting the security and integrity of those data.

4. Clarification and communication of roles in data classification are responsibilities of the DoIT Administrative Systems Team committee at the University.

5. Revision History

   None

6. Approval and Effective Date

Approved: ______________________________ 10/11/2016
Dr. Gabriel Fagbeyiro, AVP/CIO Date

Approved: Ray L. Belton 10-27-16
Dr. Ray Belton, President/Chancellor Date