University Policy 5.2: Data, Information Access and Security

Executive Summary

The purpose of this policy is to provide general guidance on the protection of University data and information being processed by manual as well as automated systems. The policy also sets forth the responsibilities for data and information security for all individuals and departments at Alabama A&M University that access, process, or has custody of University data.

I. Purpose

The purpose of this Policy is to provide general guidance on the protection of University Data being processed by manual and automated systems, and to describe the responsibilities of the Provost/Vice Presidents, and of custodians, managers and users of University Data for protecting the records and reports generated by these information processing systems.

II. Definitions

For the purposes of this Policy:

A. An "**Information Custodian**" is an individual designated with control over and responsibility for a specific set of University Data.
B. An "**Information Manager**" is an individual or office designated by an Information Custodian to maintain security controls over a specific set of University Data.
C. An "**Information User**" is anyone using University Data as a part of his or her job or another University-related activity.
D. "**University Data**" is defined as all information content related to the business of the University that exists in electronic, digital or paper form. The degree of protection required for different types of University Data is based on the nature of the data and compliance requirements. The following three classification levels will be used for classifying University data:

    1. **Confidential Data:** Confidential Data is University Data for which unauthorized disclosure or unauthorized modification would result in significant financial loss to the University, impair its ability to conduct business, or result in a violation of contractual agreements or federal or state laws or regulations, including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), the State Personnel Act, the Federal Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry Data Security Standard (PCI DSS). *Examples: Social Security Numbers, payment card numbers, medical records, student data that is not considered directory information, information protected by non-disclosure agreements, confidential research data.*

2. **Sensitive Data**: Sensitive Data is University Data for which unauthorized disclosure or unauthorized modification would not result in direct financial loss or any legal, contractual or regulatory violations, but may otherwise adversely impact the University. Sensitive Data is generally intended for use within the University or within a specific unit, department or group of individuals with a legitimate need-to-know. *Examples: Budget and salary information, personal pager or cell phone numbers, departmental policies and procedures, internal memos, incomplete or unpublished research.*

3. **Public Data**: Public Data is University Data that has been explicitly approved for distribution to the public by the Information Custodian or through some other valid authority. Disclosure of Public Data requires no authorization and may be freely disseminated without potential harm to the University. *Examples: Advertising, product and service information, directory listings, published research, presentations or papers, job postings, press releases.*

III. Policy

Information is a vital component of University operations, and it is important to ensure that persons with a need for information have ready access to that information. It is equally important to ensure that measures have been taken to protect critical information against accidental or unauthorized access, modification, disclosure or destruction, in order to ensure the security, reliability, integrity and availability of information. In addition, federal and state laws and regulations assign legal responsibility for the correct and appropriate use of information in order to protect a person's right to privacy.

This policy sets forth the responsibilities for University Data and information security for all individuals and departments at Alabama A&M University who access, process or have custody of University Data.

IV. Responsibilities

A. The **Provost/Vice Presidents** will ensure that the standards for data security that affect their respective areas of responsibility are effectively implemented. The administrative duties associated with this responsibility will be assigned by the Provost/Vice Presidents to designated Information Custodians, who typically are the managers responsible for the creation or collection of specified University Data.

B. **Information Custodians** are primarily responsible for ensuring the quality of and control over the University Data in their custody. Areas of responsibility for an Information Custodian include:
   1. Maintaining the accuracy and completeness of University Data for which he or she is responsible, whether that data be contained in the centrally managed system or in locally managed systems;

2. Classifying University Data as Confidential Data, Sensitive Data or Public Data in accordance with the definitions set forth in Section II above;
3. Determining and documenting the requirements for authorizing or de-authorizing individual access to University Data in the custody of the Information Custodian;
4. Conducting and documenting a semi-annual review to verify that individuals who have been granted access to University Data in the custody of the Information Custodian still require that access;
5. Identifying and minimizing risks and vulnerabilities;
6. Documenting and communicating information protection procedures to Information Users that have been granted access to University Data in the custody of the Information Custodian;
7. Evaluating the effectiveness of security controls related to University Data in the custody of the Information Custodian;
8. Identifying and designating Information Managers to implement security controls for the University Data in the custody of the Information Custodian; and
9. Notifying the Information and Technology Services Security Officer or other appropriate University personnel in the event of a policy violation or of a potential or actual security breach.

C. **Information Managers** are tasked with the responsibility of maintaining security controls established by University policy or guidelines or by Information Custodians. Typical Information Manager responsibilities include:

1. Collaborating with Information Technology Services to ensure that systems containing confidential or sensitive University Data employ the University's central authentication service;
2. Monitoring compliance with University policies and guidelines designed to protect University Data from unauthorized access or disclosure;
3. Administering Information Custodian-specific business and information protection controls, including information access control;
4. Providing backup and recovery of University Data;
5. Detecting and responding to security violations and vulnerabilities; and
6. Being aware of all relevant University policies and guidelines regarding University Data, including, but not limited to, the Supplemental Regulations to this Policy; and
7. Reporting any suspected or actual policy violations, security breaches or security vulnerabilities to the Information Custodian.

D. **Information Users** include all persons who have been authorized to read, write or update University Data. Information Users are responsible for:

1. Using University Data in accordance with University policies and guidelines;
2. Maintaining security appropriate for the classification level of University Data during processing or storage of that data;

3. Complying with all security controls established by the Information Custodian and/or Information Manager;
4. Avoiding disclosure of Confidential Data or Sensitive Data to unauthorized persons without the permission of the Information Custodian or Provost/Vice President; and
5. Annually identifying any new databases or information systems which have been created or acquired by them for use by more than one person and that contain Confidential Data or Sensitive Data, and reporting such databases or systems to the appropriate Information Custodian.

V. Implementation

The Chief Information Officer (CIO) for the Division of Information Technology Services is responsible for developing security procedures and guidelines pursuant to this Policy, ensuring that such procedures and guidelines are published and distributed to all Information Users, and conducting periodic reviews of such procedures and guidelines. This Policy and all supporting procedures and guidelines will serve as the standards of information and data security to be applied by Information Custodians, Information Managers and Information Users and will be the basis for compliance monitoring, review and audit.

VI. Compliance

Failure to comply with this Policy and/or regulations promulgated hereunder will be deemed a violation of University Policy and subject to disciplinary action in accordance with the disciplinary guidelines as outlined in the Faculty or Staff Handbook, whichever one is applicable to the individual.

Revision History

- Initially approved: December 2011 (Procedure Approved)
- December 2012 (Board Approved as Policy)

Authority: President

Responsible Office: Information Technology Services