Purpose

The purpose of this policy is to assist The University of Alabama community in the classification and protection requirements for all information. Based on the classification of the information, users are required to implement and follow appropriate security control procedures. Having information appropriately classified will enable automated management in University systems that utilize classifications.

Policy

All University of Alabama (UA) information stored, processed, or transmitted must be classified in accordance with this policy. Based on classification, users are required to implement appropriate security controls for the protection of the information, and follow the Information Protection Procedure.

All University information must be classified into one of the three following categories:

- **Public information**: Information that may be disclosed to the general public without an expectation of harm, and consistent with other applicable University policy.
  - Examples: public phone directory, course catalogs, public research findings, enrollment figures, public websites, general benefits information, press releases, newsletters, etc.

- **Sensitive Information**: Information that should be kept confidential. Access to this information requires prior authorization and legitimate need-to-know. Privacy may be required by law or contract.
  - Sensitive information includes, but is not limited to non-directory information covered by the Family Educational Rights and Privacy Act (FERPA), budgetary plans, proprietary business plans, patent pending information, any other information whose privacy is protected by law, etc.

- **Restricted Information**: Information that is highly confidential in nature, carries significant risk from unauthorized access, or uninterrupted accessibility is critical to UA operations. Privacy and security controls are typically required by law or contract.
  - Restricted information includes, but is not limited to: social security numbers, medical information, financial information, government issued identification information, and access information including user name or email address in combination with a password or security question and answer, or security code, access code, expiration information or PIN that would permit access to an online account that is reasonably likely to contain or is used to obtain restricted information.
  - Laws and regulations include, but are not limited to:
    - Alabama Data Breach Notification Act of 2018 and other applicable breach notification laws
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Health Information Technology for Economic and Clinical Health (HITECH)
    - Gramm-Leach-Bliley Act (GLB Act or GLBA)
    - Payment Card Industry Data Security Standards (PCI DSS)
- Federal Information Security Management Act (FISMA)
- General Data Protection Regulation (GDPR) and other international privacy laws and regulations

Classification of Research Data
For the classification of human subject research information and/or export control information, refer to the Research and Economic Development Institutional Review Board (IRB) website.

Responsibilities
University divisions that own sensitive and restricted information must name a data steward for its information. The data steward must grant formal approval for the access and use of its sensitive and restricted information.

Specific roles and responsibilities for protecting UA information

1. **Data Stewards** have administrative control and are officially accountable for specific information. Data stewards shall:
   - Define the System of Record (SOR),
   - Assign an appropriate classification to the information,
   - Govern processes for determining access to information,
   - Ensure compliance with policies and regulatory requirements related to the information, and
   - Oversee risk assessment and analysis

2. **Data Custodians** protect the information on behalf of the data steward.
   - OIT along with departmental units must be responsible for protecting all UA information maintained/stored in the UA information systems.
   - Distributed Information Technology (IT) units must be responsible for protecting all information maintained/stored in unit level information systems.
   - Database administrators are data custodians that have direct access to and management of UA information.
   - System administrators are data custodians within OIT or college/department units with day-to-day responsibility for maintaining information systems and the information contained within.

3. **OIT Information Security**
   - Members of the OIT Security Team are responsible for developing and implementing an information security program as well as the supporting information security and protection policies, standards and procedures.

4. **Security and Infrastructure Liaison – IT Forum**
   - Each college or department senior manager will designate at least one security and infrastructure individual who will act as a liaison to the IT Forum.
   - Liaisons oversee information security responsibilities for the college/department units, including assisting with security awareness and security incident response.

5. **Users**
   - Users are individuals authorized to access University information and are responsible for protecting information on a daily basis through adherence to University policies.
   - All users with access to University information are required to protect information appropriately.

Incident Reporting and Management
Any suspected breach or compromise of sensitive or restricted information must be reported immediately to the Information Security Office in the Office of the Vice Provost and Chief Information Officer (CIO) for Information Technology and to the dean or administrative unit head. Specific procedures for reporting a suspected or actual breach/compromise of information are located on the Information Security website, and include other offices that must
also be notified immediately. Upon receiving the report, the Information Security Office will be responsible for conducting or coordinating the investigation, making or assessing recommendations for corrective action, reporting the incident to the Executive Computer Incident Response Team (ECIRT) and other administrative units as needed, and maintaining documentation of the incident.

Protection Requirements Based on Classification
The University of Alabama Information Protection Procedure document defines minimum protection requirements for each classification category of information when being used or handled in a specific context (e.g., sensitive information sent in an email message). Please note that these protections are not intended to supersede any regulatory or contractual requirements for handling information.

Definitions

Chief Information Security Officer (CISO): A designated individual responsible for the management of information security for the entire campus.

Classification (Information classification): Information classification is the process of sorting and categorizing information into various types, forms or any other distinct class. Information classification enables the separation and classification of information according to data set requirements for various business or personal objectives. It is mainly an information management process and allows enablement of protection requirements based on classification.

Data Custodian: A data custodian is an employee of the University who has administrative and/or operational responsibility over UA information. In many cases, there will be multiple data custodians over a single piece of data. An enterprise application may have teams of data custodians, each responsible for varying functions.

Data Steward: A data steward is a role within an organization responsible for utilizing some portion of the University's information governance processes to ensure fitness of data elements - both the content and metadata.

Export Controls: Export-controlled information or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulations (EAR). Export-controlled information must be controlled as restricted information and marked accordingly.

Financial Information: Nonpublic information referring to an individual’s assets, liabilities, credit, financial account numbers including bank, savings, credit or debit with or without balances, transactional information, social security numbers and or other tax identification numbers.

Health Information Technology for Economic and Clinical Health Act (HITECH): Federal regulation enacted under Title XIII of the American Recovery and Reinvestment Act of 2009. The HITECH Act was created to promote and expand the adoption of health information technology, specifically, the use of electronic health records (EHRs) by healthcare providers.

Health Insurance Portability and Accountability Act (HIPAA): Federal regulation that defines the management of protected health information held by covered entities and/or business associates of covered entities.

Medical Information: any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment or diagnosis by a health care professional. Any information containing an individual’s health insurance policy numbers, subscriber identification number, or any unique identifier used by a health insurer.
**Risk Analysis:** An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of information at defined classification levels.

**Risk:** The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact on confidentiality, integrity and availability of confidential information.

**System of Record (SOR):** The system of record is the authoritative source for a particular type of data (e.g., CWID, SSN, student discipline records, payroll information, academic transcripts, etc.). To ensure information integrity, there must be one -- and only one -- system of record for a given type of data. System of record is a data management term for an information storage system commonly implemented on a computer system running a data base management.

**References**
- Information Protection Procedure

**Scope**
This policy applies to all faculty, staff, students, approved volunteers, or contractors who have access to University information.

---

**Office of the Provost**

Signed: 

Joel Brouwer

Associate Provost

10/28/2020