



# FLORIDA A&M UNIVERSITY

## INFORMATION TECHNOLOGY SERVICES (ITS)

### Information Access Control/Handling Procedure

Information is an asset of vital importance to Florida A & M University (FAMU). FAMU's Information Technology Services (ITS) procedure is to take reasonable and appropriate steps to identify and protect information originated or owned by the University, or entrusted to the University by others. All University information, regardless of format (written, electronic, verbal), is covered by these guidelines unless specifically exempted by Executive Administration and/or the legal department in writing. Proper information classification, protection and handling are the responsibility of all University employees, including consultants, contractors and temporary employees. A part of handling information is maintaining an auditable chain of custody process of information requiring such controls. Departments are advised by ITS to identify and report stores of sensitive / confidential information as well as users roles and responsibilities in accessing University information.

#### Information Classification

##### Public Information

Public information poses no risk to the University if it is made generally available. Dissemination of this information does not require specific approval from the information owner. Public information can be viewed or copied without restriction. The decision to make a piece of information public should be deliberate and approved by the approving authority or process.

##### Internal Information

Internal Information is information whose loss, corruption or unauthorized disclosure is of importance only inside the University and, therefore, would not result in a business, financial or legal loss. Internal information requires information owner approval before being distributed. All information should be considered to be at the internal information classification unless otherwise labeled or explicitly defined in the university's information-handling guidelines.

##### Confidential Information

Confidential information is information that is intended, by the information owner, for a particular audience. This information is for use solely within the university or by its designated partners, and it is limited to those with a "need to know." The explicit approval of the information owner is required to release this information even to those with a need to know.

##### Restricted Information

Restricted Information is information, whose loss, corruption or unauthorized disclosure would severely harm the University's reputation or business position, resulting in financial, reputation and legal loss. The explicit approval of the information owner is required to release this information, even to those with a need to know. Included in this category is any information that would be considered "insider information."

The following matrix is a guideline suggested by ITS unless a department has its own approved set of procedures for labeling and handling sensitive information. Any guidelines that are created by an individual department must have those guidelines approved, in writing, by University Executive Administration and/or the legal department.

	<b>Public</b>	<b>Internal</b>	<b>Confidential</b>	<b>Restricted</b>
Electronic Storage Location	No restrictions	All except external Web and external FTP	Managed and monitored servers	University desktop/laptop, corporate file share or corporate database
Electronic Storage Protection	Unprotected	Password authentication	Validated strong passwords or multifactor authentication	Strong multipart authentication and encryption
Physical Storage Protection	No restrictions	Take reasonable precautions to restrict access	Store in a locked container; restrict access to authorized people	Store in a locked container; restrict access to authorized people
Granting of Access	READ: No restrictions UPDATE: Information owner or designee	READ: Information owner designates by role UPDATE: Information owner designates by role	READ: Information owner designates by individual UPDATE: Information owner designates by individual	READ: Information owner designates by individual UPDATE: Information owner designates by individual
Electronic Transmission <sup>1</sup>	No restrictions	Obfuscated	Encrypted	By information owner only with encryption
Destruction Method	Any	Shred or place in proprietary waste	Shred	Shred
Labeling	Must be explicitly labeled or defined as "public" in COMPANY's information classifications	All unlabeled information should be considered internal unless otherwise labeled or defined.	Label all electronic (Word, Excel, PowerPoint and others) and physical documents; use watermark option where possible in electronic documents	Label all electronic (Word, Excel, PowerPoint and others) and physical documents; use watermark option where possible in electronic documents

<sup>1</sup> Electronic Transmission - in the absence of "encryption" software the user may encode the information with a password/passphrase.

The Following laws, rules and/or regulations shall be adhered to for guidance in the enforcement of this guideline/procedure.

The **Family Educational Rights and Privacy Act of 1974**, most often referred to as **FERPA**, deals specifically with the education records of students, affording them certain rights with respect to those records. For purposes of definition, education records are those records, which are: 1) Directly related to a student, and 2) Maintained by an institution or a party acting for the institution.

**FAMU Regulation 10.129 Limited Access Records.**

**Florida Statute 501.171 Security of confidential personal information.**

Ronald E. Henry, II. Associate Vice President / Chief Information Officer

APPROVED 12/6/2017