

STANDARD ADMINISTRATIVE PROCEDURE

29.01.99.M1.29 Data Classification and Protection

Approved June 15, 2009

Next scheduled review: June 15, 2012

Standard Administrative Procedure Statement

The purpose of this SAP is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk.

Definitions

Confidential – information that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements.)

Examples of “Confidential” data may include but are not limited to:

- Personally Identifiable Information, such as: a name in combination with Social Security number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records

Custodian of an Information Resource - a person responsible for implementing owner-defined controls and access to an information resource. Custodians may include TAMU employees, vendors, and any third party acting as an agent of, or otherwise on behalf of TAMU and/or the owner.

Mission Critical Information - information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Owner of an Information Resource - a person responsible:

- For a business function; and

- For determining controls and access to information resources supporting that business function.

Public – (default classification) information intended or required for public release as described in the Texas Public Information Act.

Sensitive – an optional TAMU or owner defined category. Sensitive data that may be subject to disclosure or release under the Texas Public Information Act, but requires additional levels of protection.

Examples of sensitive data may include but are not limited to the following:

- operational information
- personnel records
- information security procedures
- research
- internal communications

Specialized Information System – systems containing embedded information technology that have been assigned a very specific task (e.g. instruments with embedded computer systems). The following information systems do not need to be documented or scanned:

- Printers
- Scanners
- Fax Machines

University Data – data that is in the possession or under the control of an individual (i.e., owner, custodian, or user) by virtue of that person’s employment or affiliation with the University.

User of an Information Resource - an individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

Responsibilities and Procedures

1. GENERAL

Data Classification provides a framework for managing data assets based on value and associated risks. It also guides the application of the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All data, whether electronic or printed, should be classified. Consistent use of data classification reinforces with users the expected level of protection of those data assets in accordance with Texas A&M Security Rules and Standard Administrative Procedures (SAP).

The purpose of this SAP is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security controls and requirements may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

2. APPLICABILITY

This SAP applies to all University Data owners, custodians, and users. It also applies to information resources storing University Data regardless of ownership of the particular storage device. Other Federal, State, or contractual requirements may be in addition to or supersede the requirements specified in this SAP.

The information resource owner or designee (e.g., custodian, user), is responsible for ensuring that the risk mitigation measures described in this SAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this SAP. All exclusions must be in accordance with SAP 29.01.99.M1.27 Exclusions from Required Risk Mitigation Measures.

3. RESPONSIBILITY

The owner of an information resource, with the concurrence of the President or Vice President and Associate Provost for Information Technology, is responsible for classifying business functional information. The University is responsible for defining all information classification categories except the “Confidential” category.

It is the responsibility of anyone (e.g., owner, custodian, user) having data in their possession or under their direct control (e.g., manages the storage device) to know the classification of the data and ensure the appropriate safeguards are in place. Anyone possessing confidential data shall ensure that appropriate risk mitigation measures (e.g., encryption) are in place to protect data from unauthorized exposure.

4. PROCEDURES

4.1 Data is to be classified as Confidential and/or Mission Critical, Sensitive, or Public (default). The classification of the electronically stored data is to be reported in the annual information security risk assessment process (ISAAC).

4.2 Access to confidential or sensitive information shall not be permitted with the use of a User ID alone (e.g., UIN only).

4.3 Where feasible, all data files are to be scanned on an annual basis to determine if those files contain SSNs. If SSNs are found or known to be present in a file, they

are to be removed or appropriate risk mitigation measures applied (e.g., encryption) if their continued presence is required. The results of the file scanning and risk mitigation measures taken shall be reported during of the annual ISAAC process. All SSNs that are to be retained and stored are to be reported to and approved by the Vice President and Associate Provost for Information Technology. The reporting and approval process will be in the manner indicated in the ISAAC process. Specialized information systems that cannot be scanned and are not capable of storing SSNs shall also be documented accordingly as part of the ISAAC process.

Related Statutes, Policies, or Requirements

Supplements [University Rule 29.01.99.M1](#)

Additional Information [Social Security Number Scanning](#), [Data Encryption](#)

Contact Office

Contact [Information Technology Issues Management](#) for SAP interpretation or clarification.

OFFICE OF RESPONSIBILITY: [Vice President and Associate Provost for Information Technology](#)
