Sam Houston State University
A Member of The Texas State University System
Information Technology Services (IT@Sam)

Data Classification Policy: IT-06

Introduction:
Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All SHSU data, whether electronic or printed, must be classified as Confidential, Agency-Sensitive, or Public. Consistent use of data classification reinforces with users the expected level of protection of SHSU data assets in accordance with SHSU policies.

The purpose of the Data Classification Policy 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 standards, which define these 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.

Scope:
The SHSU Data Classification policy applies equally to all Data Owners and Data Custodians.

Policy Statement:
Data Owners and/or Data Custodians must classify data as follows:

1. Confidential: Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act, FERPA, HIPPA) and other constitutional, statutory, judicial, and legal agreements. Examples of Confidential data may include, but are not limited to:
    a. Personally identifiable information such as a name in combination with Social Security Number (SSN) and/or financial account numbers
    b. Student education records such as posting student identifiers and grades
    c. Intellectual property such as copyrights, patents and trade secrets
    d. Medical records
2. Protected: Sensitive data that may be subject to disclosure or release under the Texas Public Information Act but requires additional levels of protection. Examples of Protected data may include but are not limited to SHSU:
    a. Operational information
    b. Personnel records
    c. Information security procedures
    d. University-related research
    e. SHSU internal communications

3. Public: Information intended or required for public release as described in the Texas Public Information Act.

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, May 15, 2011
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2014