Sam Houston State University
A Member of The Texas State University System
Information Technology

Data Classification Policy: IT-06

PURPOSE:

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, Protected, or Public. Consistent use of data classification reinforces with users the expected level of protection of Sam Houston State University (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 Information Owners and Information Custodians.

POLICY STATEMENT:

Information Owners and/or Information Custodians must classify data as follows:

1. **Confidential**: 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, HIPAA, PCI) 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**: 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.

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, April 17, 2023
Reviewed by: Heather Thielemann, Information Resources Manager, April, 2023
Next Review: April, 2024