SUL ROSS STATE UNIVERSITY

A Member of the Texas State University System

SRSU Policy: Data Classification Policy
SRSU Policy ID: APM 7.09
Policy Reviewed by: Chief Information Officer
Approval Authority: Executive Cabinet
Approval Date: April 14, 2026
Next Review Date: April 14, 2031

Purpose/Reason

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 Sul Ross State University data, whether electronic or printed, should be classified as Public, Sensitive, Confidential, or Regulated using the Data Classification Guide on the OIT website. Consistent use of data classification reinforces with users the expected level of protection of Sul Ross State University data assets in accordance with SRSU Policies.

The purpose of the Sul Ross State University 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 and Applicability

The Sul Ross State University Data Classification Standard applies equally to all individuals who use or handle any Sul Ross State University Information Resource.

Sul Ross State University data created, sent, printed, received, or stored on systems owned, leased, contracted, administered, or authorized by Sul Ross State University are the property of Sul Ross State University and its protection is the responsibility of the Sul Ross State University data owners, custodians, and users.

Policy Specifics

SRSU data created, sent, printed, received, or stored on systems owned, leased, administered, or authorized by SRSU are the property of the university and its protection is the responsibility of the data owners, custodians, and users. Data Owners must classify data according to the Data Classification Guide on the OIT website.

Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Sul Ross State University Information Resources access privileges, and to civil and criminal prosecution.

Standards

	Data Classification Levels			
	Public	**Sensitive**	**Confidential**	**Regulated**
Definitions	Information that is free and without reservation made available to the public.	Information that could be subject to release under an open records request but should be controlled to protect third parties.	Information that must be protected from unauthorized disclosure or public release (exempted from the Public Information Act), based on state or federal law or other legal agreement.	Information that is controlled by a state or federal regulation or other 3rd party agreement.
Justification	Access to some information, such as published reports, agency news, and other public related materials, does not need to be tracked or monitored. In such circumstances, it is most efficient to keep the information available for access without requiring the intervention of university employees.	Some sensitive information can be made publicly available. Such information should be vetted/verified before it is released. By protecting access to the information and requiring an open records request, Sul Ross State University ensures that the most accurate and relevant information is provided to the requestor without accidentally disclosing confidential information.	Data collected and maintained by Sul Ross State University that is protected from disclosure either through a codified exception to the Public Information Act or through opinions or decisions of the Attorney General's Public Information office. Such information may also be subject to breach notification requirements under Texas law.	Sul Ross State University interacts with the federal government or provides services that are regulated by federal rules and laws. In such instances, the information maintained by those agencies must comply with federal controls. Sometimes information collected or generated may be subject to agreements such as Non-Disclosure Agreements (NDA) and must be maintained by relevant 3rd party agreements.

Examples	Information that is published to the public website and requires no authentication • Agency publications. • Press releases • Public web postings. • Public Social Media postings.	Information subject to the public information act that can be obtained with an open records request. Such information is stated in the handbook published by the Attorney General of Texas. Additionally, information that is specific to Sul Ross State University and does not apply externally to other agencies or services. • University usernames. • University internal IP Addresses. • Gross Salary.	Information that has been exempted from public release under the Texas Government Code Ch. 552 or Information, whose public release, may result in adverse consequences to the organization. • Attorney-Client communications • Computer Vulnerability Reports • Protected draft communications • Net salary information • Combination of information defined as PII and SPI under the Texas Business and Commerce Code §521.002(a)(1) and §521.002(a)(2) that are exempted from release by the office of the Texas Attorney General.	• HIPAA Security (45 CFR Parts 164). • PCI DSS v2.0 and above. • Federal Tax Information (FTI). • Federal Insurance Contributions Act (FICA). • Non directory information defined under FERPA.
TX- Ramp Confidentiality Level	Exempt	Level 1	Level 2	Level 2
Consequence of Public Disclosure	No adverse consequences.	Loss of reputation Loss of trust.	Potential criminal or civil penalties.	Federal investigation Loss of revenue.

Exceptions

The ISO, with the approval of the Sul Ross State University President, may issue documented exceptions to controls in this standard based on justifications communicated as part of the risk assessment process.

Enforcement

- Failure to adhere to the provisions of this policy statement may result in:
    - Loss of Sul Ross State University Information Resources access privileges.
    - Disciplinary action up to and including termination for employees, contractors, or consultants.
    - Dismissal of interns and volunteers.
    - Suspension or expulsion in the case of a student.
    - Civil or criminal prosecution.

Authority and Responsibility

Questions related to this policy statement or to the appropriate use policy statement at any component institution should be addressed to the SRSU Chief Information Officer.