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: 10/11/2016
Next Review Date: 10/11/2021

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 or Confidential, 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 Policy applies equally to all individuals who use or handle any Sul Ross State University Information Resource.

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.

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.