Sul Ross State University
Position Description

Official Title: Information Security Officer Job Code: 3801
Salary Group: Unclassified 4

Summary
Function: The Information Security Officer develops, implements and maintains a clear and comprehensive Information Security Plan that incorporates and is not limited to: Security Policy and Compliance, Security Awareness, Security Risk Assessment and Mitigation, Security Incident Response, and Information Assurance with respect to Disaster Recovery and Business Continuity.

Scope: Responsible for the Information Security Plan for all Sul Ross State University campuses.

Duties
Essential:

- developing, recommending and maintaining an institution-wide information security plan as required by §2054.133, Texas Government Code;
- developing, recommending and maintaining information security policies and procedures that address the requirements of TAC 202 and the institution's information security risks;
- working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of TAC 202 and the institution's information security risks;
- providing guidance and assistance to senior institution of higher education officials, information owners, information custodians, and end users concerning their responsibilities under TAC 202;
- ensuring that annual information security risk assessments are performed and documented by information-owners;
- reviewing the institution's inventory of information systems and related ownership and responsibilities;
- developing and recommending policies and establishing procedures and practices, in cooperation with the institution Information Resources Manager (IRM), information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure;
- coordinating the review of the data security requirements, specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data;
- verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data;

- reporting, at least annually, to the state institution of higher education head the status and effectiveness of security controls;
- informing head of the state institution or the IRM in the event of noncompliance with TAC 202 and/or with the institution's information security policies.
- promoting and implementing a variety of educational programs and resources to enhance the security awareness, knowledge and consciousness of all user constituencies;
- overseeing an ongoing risk assessment program that assures periodic evaluation of information resources (both centrally and departmentally managed) with respect to current and emerging security threats;
- developing and implementing appropriate protocols for managing, escalating, and documenting security incidents;
- collaborating in the development and maintenance of appropriate disaster recovery and business continuity plans to assure acceptable information availability and protection;
- developing, analyzing and maintaining metrics, reports and records associated with security policy violations, breaches, and similar incidents;
- pro-actively participating in security and technology groups and associations, both internal and external to the university, and pursuing other professional development activities as necessary to enhance professional knowledge and competencies;
- using elevated access privileges in an ethical and professional manner with appropriate regard for privacy and confidentiality; and,
- showing responsibility for personal safety and the safety of others; must exercise due caution and practice safe work habits at all times.

Non-Essential: Performs additional job-related duties and responsibilities as requested.

Supervision Received: Reports to the Chief Information Officer (CIO)/Institutional Resource Manager (IRM)

Supervision Given: None

Education Required:

- Associate’s Degree or other equivalent technical degree

Education Preferred:

- Bachelor’s Degree
- Documented level of security training or a certification

Experience Required:

- Experience as a security or technology administrator in a complex technology environment

Experience Preferred:

- Demonstrable experience in an information security position or role

- Prior experience as a network, server, database, or application administrator
- Experience with UNIX and UNIX shell scripting

Equipment/Skills Required:

- Strong analytical and computer skills; effective oral and written communication skills; ability to relate to individuals in a multicultural environment.
- Ability to forge and sustain effective and productive working relationships between diverse members of project teams and work groups
- Ability to communicate technical concepts and issues with both technical and non-technical individuals
- Skill in facilitation, organization, collaboration, negotiation, consultation, and communication

Equipment/Skills Preferred:

- Knowledge of authoritative standards, guidelines, and best practices relative to information security

Working Conditions

Based in Alpine; some travel required. May be required to work a flexible schedule, including nights, weekends and holidays. Exempt from overtime provisions. Position is Security Sensitive.

Date revised: May, 2015