[New policy: January 5, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.00: Information Security Roles and Responsibilities

DATE: January 5, 2018

PURPOSE: The purpose of this policy is to define roles and responsibilities for securing information and information systems.

REVIEW: This OP will be reviewed in July every five years, or as needed, by the chief information officer and appropriate personnel with recommended revisions forwarded through the vice president for finance and administration to the president by August 15 of the same year.

POLICY/PROCEDURE

1. Overview

The university operating policies for information security (OP44 series) derive from and wholly encompass the requirements and guidance in Texas Administrative Code Chapter 202 and the Security Control Standards Catalog (per TAC 202.76). Derivation of authority is marked in each policy section. ASU defines technical policy terms in the Information Technology Glossary.

2. Responsibilities and Duties
Authority-Texas Administrative Code (TAC): 202.70; 202.71; 202.72; 202.73(a)

a. The president must approve acceptance, transfer or mitigation for any system with a high residual risk.

b. The president or designated representative must:

(1) Designate an information security officer;

(2) Allocate resources sufficient to reduce risk to a level acceptable to the university president;

(3) Ensure executive support for information security;

(4) Ensure trained personnel are available to address university information security needs;

(5) Ensure executive support in development of an annual report on the state of information security to the university president;

(6) Approve the information security program annually;

(7) Ensure university strategic planning and operational processes include information security; and

(8) Formally designate information owners.

c. The information security officer (ISO) must:

(1) Have authority for information security for the entire institution;

(2) Report to executive level management;

(3) Possess the knowledge and experience necessary to administer the information security program;

(4) Have information security as primary duty, whenever possible;

(5) Maintain an institution-wide information security plan;

(6) Maintain policies that address university information security risks;

(7) Ensure that information security risk assessments are performed, controls are enhanced as needed and the results are documented by information owners;

(8) Approve acceptance, transfer or mitigation of Low or Moderate residual risks, in coordination with the information owner;

(9) Provide training and direction of personnel with information security responsibilities;

(10) Provide guidance and assistance to university executives, information owners, custodians and users on issues of information security;

(11) Ensure every university information system is formally assigned an information owner and custodian of information and information systems;

(12) In cooperation with information owners and custodians, establish policies, procedures, and guidance to prevent unauthorized or accidental modification, destruction or disclosure;

(13) Ensure controls satisfying data security requirements and recommended by information system security assessments are in place prior to implementation, contractual obligation or purchase for any high impact information systems or those information systems that will receive, store, or share confidential information;

(14) Report to the university president at least annually on the effectiveness of security controls, status of key initiatives, high residual risks and information security requirements and requests;

(15) Inform information owners and custodians in the event controls, policies, or procedures are not compliant with regulatory requirements or university policies; and

(16) Issue exceptions to information security requirements or controls, with the approval of the university president or designated representative.

d. Information owners or their designated representative must:

(1) Classify information under their authority in accordance with the university's established data classification categories;

(2) Approve access to information systems and periodically review access lists based on information system risk posture;

(3) Assign custody of university information and information systems, communicate appropriate security controls and provide sufficient authority and resources to custodians to implement security controls;

(4) Coordinates information security requirements with the ISO;

(5) Be accountable for all exceptions to security controls;

(6) Ensure exceptions to security controls are justified and documented, and approval obtained from the ISO; and

(7) Participate in risk assessments under the guidance of the ISO.

e. Custodians must:

(1) Implement controls as required by the information owner and ISO;

(2) Help information owners evaluate the cost-effectiveness of controls;

(3) Must detect, report, and investigate incidents using guidance approved by the ISO;

(4) Contribute information needed to provide appropriate information security training to users; and

(5) Ensure information is recoverable.

f. Users must:

(1) Use information and information systems only for the purpose specified by the university;

(2) Comply with all information security controls, university policies, and regulatory requirements; and

(3) Formally acknowledge that they will comply with all university information security policies, controls and procedures.

3. Institution Reporting
Authority-TAC: 202.73(b)

a. The ISO must promptly report urgent security incidents to the Texas Department of Information Resources (DIR) (see OP 44.09).

b. ASU must report summary security incident information monthly to DIR.

c. ASU must submit a biennial information security plan to DIR.

4. Information Security Program
Authority-TAC: 202.74

a. ASU must develop an information security program that uses controls based on risk to ensure that university information systems are protected throughout the life cycle of the system and includes:

(1) Periodic risk assessments;

(2) Controls, standards and procedures that are based on risk and security assessments, cost-effectively reduce risk, address information security across life cycle of the information system, and ensure compliance with state regulation, university requirements and the DIR control standards catalog;

(3) Strategies to address risk to high impact information systems;

(4) Plans to protect facilities and other underlying technology infrastructure;

(5) Processes to remediate deficiencies; and

(6) Processes to grant exceptions.

b. The university must implement an information security program that ensures that information security controls protect university information systems throughout the life cycle of each information system based on risk posture.

c. As part of the information security program, ASU must define information classification categories (see data classification standard), administer an ongoing information security awareness program for all users (see OP 44.03), and introduce security awareness to new employees during the onboarding process (see OP 44.03).

5. Risk Management
Authority-TAC: 202.75; 202.76

a. A risk assessment of the university information and information systems shall be performed and documented as follows:

(1) The inherent impact will be ranked, at a minimum, as High, Moderate, or Low and be performed annually for High and at least biennially for Moderate and Low.

(2) Risk assessment results and similar information shall be documented and presented as required in the Risk Management Program;

(3) The ISO is responsible for accepting Low or Moderate residual risks, in coordination with the information owner. The university president is responsible for accepting risk for all systems identified with a High residual risk; and

(4) Implementation of controls to reduce risk must balance cost and effectiveness while still reducing residual risk to an acceptable level.

b. The president or designated representative may authorize more stringent standards than DIR prescribes, that also accomplishes the following:

(1) Cost-effective application of security controls for university information and information systems;

(2) Wholly contains the applicable DIR standards;

(3) Remains consistent with all applicable law, policies and guidelines; and

(4) Adequately protects information held by the university.