[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.15: Program Management

DATE: June 21, 2018

PURPOSE: The purpose of this policy is to define information security controls around program management.

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. Definition

ASU defines technical policy terms in the information technology glossary.

2. Information Security Program Plan
Authority-DIR Controls Catalog (CC): PM-1

a. ASU must develop and maintain an institution-wide information security program that:

(1) Lists the requirements for the program;

(2) Describes management and administration of the program;

(3) Identifies roles and responsibilities of the program;

(4) Is approved by the university president or designated representative;

(5) Is regularly reviewed and updated to address organizational needs; and

(6) Is protected from unauthorized disclosure or modification.

b. ASU must document the methods and philosophies employed to ensure university information systems are well managed and secure.

c. ASU must incorporate tenets of governance, risk management and compliance frameworks into the university's information program.

d. The university president is responsible and accountable for risks incurred to all university operations.

e. University senior leaders are responsible and accountable for risks incurred to university operations under their purview.

3. Senior Information Security Officer
Authority- DIR CC: PM-2

a. The university president or designated representative must designate an information security officer whose primary responsibility is the administration of the university Information Security Program.

4. Information Security Resources
Authority-DIR CC: PM-3

a. ASU uses the project and portfolio management cycle to plan information security expenditures.

b. ASU must document information security expenditure planning during the project and portfolio management cycle.

c. The ASU project and portfolio management cycle ensures that information security resources are spent as planned.

d. ASU must ensure information security program requirements are funded at a level to reduce risk to an appropriate level.

5. Plan of Action and Milestones Process
Authority-DIR CC: PM-4

a. ASU must put security initiatives into the project portfolio to be prioritized with other technology initiatives.

b. ASU must determine and make needed control enhancements identified during security and risk assessments.

6. Information System Inventory
Authority-DIR CC: PM-5

a. ASU must develop and maintain an inventory of all university information systems across their lifecycle at the university.

7. Information Security Measures of Performance
Authority-DIR CC: PM-6

a. ASU must develop, measure and report on the effectiveness of information security controls and performance measures.

b. The ISO must make security program updates to the CIO at least quarterly.

8. Enterprise Architecture
Authority-DIR CC: PM-7

a. ASU must build its enterprise architecture using principles of information security to ensure operational effectiveness and a cost-balanced reduction of risk.

b. ASU must ensure information security is appropriately addressed in the university's governance, risk and compliance processes.

9. Threat Awareness Program
Authority-DIR CC: PM-16

a. ASU must share notifications of information security threats with constituents that would be most likely affected.

b. ASU must send general notifications of seasonal threats to the campus community.

c. The ISO must engage community resources to maintain awareness of the threat landscape.

d. ASU must notify DIR of any local security incidents that may affect other state agencies.