[New policy: January 5, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.19: System and Services Acquisition

DATE: January 5, 2018

PURPOSE: The purpose of this policy is to define information security controls around system and services acquisition.

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. System and Services Acquisition Policy and Procedures
Authority-DIR Controls Catalog (CC): SA-1

a. ASU must identify, document and address security requirements during all phases of information system development or acquisition while carefully weighing costs against operational requirements.

3. Allocation of Resources
Authority- DIR CC: SA-2

a. ASU must allocate sufficient and appropriate resources (including capital planning and investment control process) to support information security requirements across the lifecycle of an information system.

b. ASU must establish a discrete budgetary line item for information security.

4. System Development Lifecycle
Authority-DIR CC: SA-3

a. ASU must manage information security requirements, security testing and audit controls across the development and/or acquisition lifecycle of university information systems.

b. ASU must define and assign roles and responsibilities for managing information security requirements across the lifecycle of university information systems.

c. ASU must keep test environments physically or logically separate from production environments except in cases where the risk to production information is low.

[New policy: January 5, 2018]

5. Acquisition Process
Authority-DIR CC: SA-4

a. ASU must ensure security requirements for information systems are included in contracts (see OP 30 series and the IT Contract Review Process).

b. ASU varies security strength requirements based on system risk posture.

6. Information System Documentation
Authority-DIR CC: SA-5

a. ASU must obtain, protect and make available to authorized personnel adequate documentation to secure university information systems.

7. External Information System Services
Authority-DIR CC: SA-9

a. ASU must require vendors secure university information systems and information under their control to the level required by risk posture.

b. Custodians must monitor cloud services and report security discrepancies to vendors for correction.

8. Developer Configuration Management
Authority-DIR CC: SA-10

a. ASU information owners must approve security-related information system changes through a formal change management process prior to implementation.

b. Using a formal change management process, ASU must correct security flaws in information systems as soon as practical considering risk posture.