[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.05: Security Assessment and Authorization

DATE: June 21, 2018

PURPOSE: The purpose of this policy is to define information security controls around security assessment and authorization.

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. Security Assessment and Authorization Policy and Procedures
Authority-DIR Controls Catalog (CC): CA-1

a. ASU must have an Information Security Program that assesses and enhances the information security posture of the university through use of security assessment and risk assessment processes.

b. ASU must manage and protect the confidentiality, integrity, and availability of information systems based on sensitivity and risk.

c. Selection and application of controls will consider the cost, sensitivity of the university information, risk, and appropriate time in which to complete remediation.

3. Security Assessments
Authority- Texas Administrative Code (TAC) 202.76(c), DIR CC: CA-2

a. ASU must annually review information security policies and controls to assess effectiveness.

b. Risks are accepted or mitigated.

c. ASU must assign action items and add an estimate of work to the assessment.

d. The university president or designated representative must engage an independent contractor to review the ASU information security program for compliance with Texas Administrative Code 202 at least biennially.

4. System Interconnections
Authority-DIR CC: CA-3

a. ASU must authorize all connections from university information systems to information systems outside of the university.

b. ASU will use contracts as security connection agreements to ensure security controls of external parties are the same or better than local security controls.

c. The ISO must approve any connections made to external parties.

d. ASU will monitor external parties for compliance with required security controls.

5. Plan of Action and Milestones
Authority-DIR CC: CA-5

a. ASU must track information security control deficiencies.

b. ASU must assign and track actions to remediate security control deficiencies.

c. ASU must complete remediation or mitigation in a cost-effective and timely manner.

6. Security Authorization
Authority-DIR CC: CA-6

a. The information owner or designated representative must approve an information system for processing before moving into production or when making a significant change.

b. The information owner or designated representative must approve the security posture of an information system.

7. Continuous Monitoring
Authority-DIR CC: CA-7

a. ASU must monitor information systems to confirm that security practices and controls are adhered to and are effective on an ongoing basis.

b. Routine monitoring and analysis of information system controls are required on a schedule consistent with system risk.

c. Backup strategies for security logs should be consistent with security risk.

d. Logging of administrator and root access should be consistent with security risk.

e. Custodians must report any security issues discovered during log review or alerting to the ISO for follow-up investigation.

f. Under direction of the ISO, custodians must respond to any security issues discovered during log review or alerting.

8. Internal System Connections

Authority-DIR CC: CA-9

a. ASU must implement all internal information system connections through the university's formal change process.

b. Custodians must configure information systems in a secure manner prior to connecting to ASU networks.

c. Custodians must gain approval from the ISO for any connections between systems that handle sensitive information.