[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.16: Risk Assessment

DATE: June 21, 2018

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

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. Risk Assessment Policy and Procedures
Authority-DIR Controls Catalog (CC): RA-1

a. ASU must have a risk management program that defines policy and directs the completion of risk assessments on information systems including identifying, evaluating and documenting the level of impact of actualization of those risks.

b. The university president or their designated representative must approve the risk management program.

c. ASU must review the risk management program at least annually.

3. Security Categorization
Authority- DIR CC: RA-2

a. In coordination with information owners, the ISO must create and update a data classification standard which describes both the information to be protected and methods required by law (or as stipulated by the information owner) for storage, transmission, and use.

b. Information owners must classify the information under the information owner's control using the university's data classification standard.

c. Information owners must approve the risk posture of systems used to process and store information governed by the information owner.

d. Information owners must include regulatory requirements in organizational procedures and implementations to protect the confidentiality, integrity and availability of university held information under the information owner's purview.

4. Risk Assessment
Authority-DIR CC: RA-3

a. ASU must conduct and document information security risk assessments based on inherent risk, sensitivity and value of information and the information system.

b. ASU must rank risk as High, Moderate, or Low and perform biennial assessments for Moderate and Low risks and annual assessments for High risks.

c. ASU must rank initial residual risk for information systems containing Category 1 information as high before application of controls.

d. ASU must document, update and report risk assessment results to the ISO.

e. In the event of the information owner and ISO cannot reach an agreement, the ISO must escalate the final risk management decision to the university president or their designated representative.

f. Information owners and custodians must report any changes to systems they control that might impact the system's risk posture to the ISO.

g. ASU must balance cost and effectiveness of implementation of controls to reduce residual risk to an acceptable level.

5. Vulnerability Scanning
Authority-DIR CC: RA-5

a. The Office of Information Technology must conduct vulnerability scans at least annually or when significant new vulnerabilities affecting an information system are identified and reported.

b. The Office of Information Technology must conduct external penetration tests at least annually.

c. The ISO analyzes vulnerability scan results to find legitimate vulnerabilities.

d. In coordination with the ISO, the custodian determines the best response to vulnerabilities found.

e. The ISO tracks vulnerability remediation.