[New policy: January 5, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.07: Contingency Planning

DATE: January 5, 2018

PURPOSE: The purpose of this policy is to define information security controls around contingency planning.

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. Contingency Planning Policy and Procedures
Authority-DIR Controls Catalog (CC): CP-1

a. ASU must create and distribute a plan for restoration of university operations that address critical information systems to minimize the impact of any significant disruption.

b. ASU must implement procedures to facilitate information systems recovery planning.

3. Contingency Plan
Authority- DIR CC: CP-2

The ASU IT Disaster Recovery Plan details implementation of the following policy elements:

a. ASU must create and securely distribute a plan which includes:

(1) Systematic assessment of potential impacts;

(2) Description of the balance between cost of preventive measures and potential loss;

(3) Description of testing and maintenance of the plan; and

(4) A documented disaster recovery plan.

b. ASU must plan for business disruption of information systems by:

(1) Identifying mission-critical functions,

(2) Providing recovery objectives,

(3) Addressing roles,

(4) Addressing interim functionality,

(5) Addressing communication, and

(6) Designating an update process.

4. Contingency Training
Authority-DIR CC: CP-3

a. ASU must provide training to users, custodians, and information owners pertinent to their role in disaster recovery.

b. ASU must conduct role-based training for disaster recovery annually.

5. Contingency Plan Testing
Authority-DIR CC: CP-4

a. The ASU disaster recovery plan must contain a provision for annual testing.

b. ASU must test disaster recovery of critical information systems at least annually.

c. Non-business critical systems must be tested based on risk assessments.

6. Alternate Storage Site
Authority-DIR CC: CP-6

a. ASU must store a copy of mission-critical university information off-site using a cost-balanced approach.

b. ASU must ensure information security controls at off-site storage facilities meet or exceed university information security controls including physical security and environmental control.

7. Information System Backup
Authority-DIR CC: CP-9

a. ASU must backup information on centralized information systems (including system state information) at a frequency based on risk posture.

b. ASU must perform system backups to a sufficient level to ensure the least disruption to university operations.

c. ASU must provide users a way to backup critical user-level information.

d. ASU must protect backups at the same level as operational information including physical security and access controls where the media is stored.

e. ASU must ensure information is available by testing restores.

[New policy: January 5, 2018]

8. Information System Recovery and Reconstitution
Authority-DIR CC: CP-10

a. ASU must ensure university information is not lost by using redundant and high availability architectures.

b. In the event of system loss or failure, ASU must recover information systems to a known secure state.