[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.17: System and Communications Protection

DATE: June 21, 2018

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

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 Communications Protection Policy and Procedures
Authority-DIR Controls Catalog (CC): SC-1

a. ASU must have an organized written response to ensure university information, communications and associated systems are protected using a variety of controls pertinent to the risk posture of the systems.

b. ASU must regularly and periodically review and update controls and procedures used to protect university information, communications and associated systems.

3. Denial of Service Protection
Authority- DIR CC: SC-5

a. ASU must structure, monitor and maintain university networks and information systems to reduce the impact of issues affecting service availability such as:

(1) Quality of service protections;

(2) Access control lists for inter-system communication;

(3) Endpoint admission controls;

(4) ISP service controls;

(5) Network segmentation using DMZs (demilitarized zones); and

(6) Perimeter protection (firewall and IPS).

4. Boundary Protection
Authority-DIR CC: SC-7

a. ASU must monitor and control communications at external boundaries of information systems and at internal boundaries within the information system based on system risk posture.

b. ASU must establish a secure boundary for university networks using technologies such as firewalls, demilitarized zones (DMZs) and intrusion prevention systems.

c. ASU must logically separate and filter traffic between Internet available services and internal university information systems.

d. ASU must secure all connections to external networks.

e. ASU must control cross-boundary communications.

f. ASU must configure network ports for the access needed at the location.

g. ASU must ensure only authorized personnel configure or modify connectivity for university networks.

h. ASU must ensure only authorized employees and third-party contractors modify or extend the network infrastructure.

i. Users must use network connectivity only as provided by the Office of Information Technology.

5. Transmission Confidentiality and Integrity
Authority-DIR CC: SC-8

a. ASU must secure transmission of university data per guidance in the university's acceptable encryption standard and data classification standard.

6. Cryptographic Key Establishment and Management
Authority-DIR CC: SC-12

a. ASU must configure all software to securely handle and store cryptographic keys (see acceptable encryption standard).

b. Custodians must securely handle manually created cryptographic keys.

7. Cryptographic Protection
Authority-DIR CC: SC-13

a. ASU must employ cryptographic controls to protect university information in accordance with the university's acceptable encryption standard and data classification standard.

b. ASU must protect sensitive information in document imaging systems to prevent inappropriate exposure when exporting or printing those documents through appropriate compensating controls such as redaction, access control or encryption.

c. Category 1 information must not be sent via e-mail unless the message is using university-approved encryption or protected so that only the authorized recipients can view the information (see acceptable encryption standard).

d. All applications that transmit sensitive information electronically must use encrypted connections, or the information itself must be encrypted or otherwise protected while being transmitted (see acceptable encryption standard).

8. Collaborative Computing Devices
Authority-DIR CC: SC-15

a. ASU must configure information systems to control and indicate active remote session connections (collaborative computing) to local users.

9. Voice Over Internet Protocol
Authority-DIR CC: SC-19

a. Office of Information Technology must secure VoIP systems commensurate with risk posture.

b. Office of Information Technology must authorize, monitor and control university VoIP systems.

10. Secure Name/Address Resolution Service (Authoritative Source)
Authority-DIR CC: SC-20

a. ASU must protect DNS (Domain Name Service) such that systems providing name resolution assure integrity of the query response providing both the data origin and integrity artifacts along with the authoritative name resolution data.

b. ASU must ensure its DNS servers specify whether a query response is authoritative.

c. ASU must ensure child zones are available only to authorized zones and people.

11. Secure Name/Address Resolution Service (Recursive or Caching Resolver)
Authority-DIR CC: SC-21

a. ASU must use an automated mechanism that considers the authenticity of the data's origin and data integrity of the recursive DNS responses to local clients.

b. ASU must configure authoritative external DNS servers hosting ASU records to deny recursion.

12. Architecture and Provisioning for Name/Address Resolution Service
Authority-DIR CC: SC-22

a. ASU must provide redundancy information systems providing DNS.

b. ASU must ensure that internal and external DNS architecture roles are separate.

13. Process Isolation
Authority-DIR CC: SC-39

a. ASU must use operating systems or configurations that support process isolation.

b. ASU must not bypass process isolation in operating systems.