[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.06: Configuration Management

DATE: June 21, 2018

PURPOSE: The purpose of this policy is to define information security controls around configuration management.

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. Configuration Management Policy and Procedures
Authority-DIR Controls Catalog (CC): CM-1

a. ASU must establish a change management program that prevents unauthorized or improper modifications to information system hardware, firmware, software, and documentation that considers the system risk posture, effect on university operations, and compliance with license agreements and intellectual property law.

b. ASU must control low-risk configuration changes through request management, incident management and system logging (see OP 44.04).

3. Baseline Configuration
Authority- DIR CC: CM-2

a. ASU must create a baseline configuration for each information system.

b. ASU must ensure the baseline configuration stays current.

4. Configuration Change Control
Authority-DIR CC: CM-3

a. ASU must maintain a change management process.

b. The change management process must:

(1) Document risks for each proposed change;

(2) Obtain approval of the ISO for changes with a security impact;

(3) Document the change and retain records of the change for at least two years;

(4) Establish appropriate testing before the change;

(5) Document a back-out plan before the change;

(6) Audit and review the change after completed; and

(7) Coordinate change activities through the change management board in its weekly meetings.

5. Security Impact Analysis
Authority-DIR CC: CM-4

a. Information owners must approve changes that affect security on information systems.

b. Custodians must obtain approval prior to implementation of changes that affect security on information systems.

6. Configuration Settings
Authority-DIR CC: CM-6

a. ASU must establish, implement and document a mandatory minimally acceptable baseline of security settings based on the system's risk posture.

b. ASU must set the most restrictive security settings consistent with operational requirements and the system's risk posture.

c. ASU must apply the baseline security settings to all information systems.

d. ASU must apply the baseline security settings to all components of the information system.

7. Least Functionality
Authority-DIR CC: CM-7

a. ASU must ensure information system configurations provide only essential services.

b. For internet facing systems, ASU must configure only those ports, services, and protocols required for university business.

c. Custodians must change factory-installed settings prior to putting information systems into production.

8. Information System Component Inventory
Authority-DIR CC: CM-8

a. ASU must document and maintain a configuration management database that includes a current inventory of each information system's components and relevant ownership information.

b. ASU must review the configuration management database at least annually.

9. Software Usage Restrictions
Authority-DIR CC: CM-10

a. ASU must use software and associated documentation in accordance with contract agreements and copyright laws.

b. ASU must track and properly license software and documentation (based on quantity, concurrent, site, or per system licensing) used on university-owned systems.

c. ASU must follow license agreements when making copies of software licensed by the university.

d. ASU must remove inappropriately licensed software from university-owned systems.

e. ASU must comply with intellectual property concerns including peer-to-peer file sharing technologies as covered in the HEOA and other legislation and regulations by blocking inappropriate use, taking corrective action, and documenting incidents.

10. User Installed Software
Authority-DIR CC: CM-11

ASU must control installation of software on systems by users via the following processes:

a. ASU must limit administrative access to labs, podiums, and servers.

b. ASU allows administrative access for users to only individually assigned workstations within their department.