[New policy: January 5, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.18: System and Information Integrity

DATE: January 5, 2018

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

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 Information Integrity Policy and Procedures
Authority-DIR Controls Catalog (CC): SI-1

a. ASU must assure the integrity of data, its source, its destination, and processes applied to the data.

b. Custodians must configure systems such that only authorized persons, processes or applications can change information in an authorized manner.

3. Flaw Remediation
Authority- DIR CC: SI-2

a. ASU must identify and report flaws in information systems (see OP 44.04 and 44.09).

b. ASU must correct vulnerabilities after they are identified within a timeframe appropriate to the criticality of the system and impact of the flaw on operations.

c. ASU must patch information systems within a timeframe determined by risk posture.

d. ASU must test patches for effectiveness and to reduce impact to operations.

e. ASU must incorporate patch management into its operational processes.

[New policy: January 5, 2018]

4. Malicious Code Protection
Authority-DIR CC: SI-3

a. ASU must employ malicious code protections on information systems and at other locations on the network based on system risk posture.

b. ASU must configure antimalware software to perform periodic scans and respond to detection of malicious code appropriately.

c. ASU must respond to false positive identification of malicious code.

5. Information System Monitoring
Authority-DIR CC: SI-4

a. ASU must monitor information systems for unauthorized access or activity.

b. ASU must monitor services for availability.

c. ASU must use intrusion monitoring tools and secure information obtained from these tools.

d. ASU must respond to unauthorized access or activity on information systems.

e. By using university information systems, users consent to monitoring, logging and reporting on their use of university resources.

f. ASU must implement a perimeter security strategy (see OP 44.17, Boundary Protection).

6. Security Alerts, Advisories, and Directives
Authority-DIR CC: SI-5

a. Custodians must monitor vendor feeds for information security information on products they support and issue alerts to information owners and users as appropriate.

b. The ISO and information owners must monitor higher education community sources, and other intelligence sources, for alerts to vulnerabilities and current potentially malicious activity, and then issue alerts to appropriate parties (see OP 44.15).

7. Spam Protection
Authority-DIR CC: SI-8

a. ASU must use appropriate technology to reduce the impact of spam email on university operations.

b. ASU must ensure all email is processed to reduce incidents of malicious activity through university controlled email gateways.

8. Information Output Handling and Retention
Authority-DIR CC: SI-12

a. Users must follow ASU records retention policies regarding retention of information (see OP 02.07).

[New policy: January 5, 2018]

b. ASU must handle and retain university information in accordance with laws and regulations.