[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.04: Audit and Accountability

DATE: June 21, 2018

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

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. Audit and Accountability Policy and Procedures
Authority-DIR Controls Catalog (CC): AU-1

a. ASU must define purpose, scope, roles, responsibilities, and compliance requirements regarding audit.

b. ASU must monitor system logs for security and operational events including user access events that might lead to inappropriate access or impact to availability.

3. Audit Events
Authority- DIR CC: AU-2

a. Where possible, on all systems requiring authentication, ASU must audit events sufficient to establish individual accountability for any action taken within the information system.

b. ASU records connection, authentication, and access events as these are most pertinent to post-event investigations.

c. For information systems containing sensitive information, ASU must ensure the recording of events that affect confidentiality.

d. ASU must maintain audit logs of changes to mission-critical systems and security infrastructure.

e. Based on risk posture, ASU must maintain audit trails sufficient to determine all activities of an individual through a system.

f. ASU must enhance the detail captured in audited events as investigations reveal necessary changes.

4. Content of Records
Authority-DIR CC: AU-3

a. Where possible, ASU must configure system audit records to include:

(1) Date/time of the event;

(2) Component of the information system where the event occurred;

(3) Description of event;

(4) Identity of subject/user; and

(5) The outcome (success or failure) of the event.

b. Events should contain all information needed to determine the logical location of the user.

5. Audit Storage Capacity
Authority-DIR CC: AU-4

a. ASU must provide local storage for security event logs.

b. For critical and high volume logs, separate storage may be used.

c. ASU must protect the auditing process by ensuring sufficient storage is available.

6. Response to Audit Processing Failures
Authority-DIR CC: AU-5

a. Where possible, ASU must detect when logging has failed and report the failure to appropriate administrative personnel via automated alerting.

b. ASU must remediate logging discrepancies.

7. Audit Review, Analysis and Reporting
Authority-DIR CC: AU-6

a. ASU continuously reviews and analyzes system logs for security and operational events (i.e., inappropriate activity, suspected violations, or unusual or otherwise suspicious activity) that might lead to inappropriate access or impact to availability.

b. Custodians must investigate suspicious activity, take corrective action, or escalate to appropriate personnel on events identified during system log reviews or from automated alerting.

8. Time Stamps
Authority-DIR CC: AU-8

a. Custodians must synchronize ASU information systems with a pool of global clock sources.

b. Where possible, audit log entries must contain a date/time stamp using local synchronized time.

9. Protection of Audit Information
Authority-DIR CC: AU-9

a. ASU must secure log and audit systems within a physically secured space and only allow access to select administrators.

b. ASU must protect audit events against unauthorized access, modification or deletion.

10. Audit Record Retention
Authority-DIR CC: AU-11

a. ASU retains audit records for a time sufficient to provide support after-the-fact security investigations and to meet regulatory and organizational information retention requirements.

11. Audit Generation
Authority-DIR CC: AU-12

a. Where possible, ASU must configure information systems to generate audit records containing information as required by policy.

b. ASU information systems must provide access control for recorded audit events.