[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.09: Incident Response

DATE: June 21, 2018

PURPOSE: The purpose of this policy is to define information security controls around incident response.

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. Incident Response Policy and Procedures
Authority-DIR Controls Catalog (CC): IR-1

a. ASU must consider the business and technical impact of an incident in determining response.

b. ASU must ensure the incident response provides a cost-effective approach to address the business and technical impact of events while protecting university information.

c. ASU must ensure incident response matches the significance of the incident.

3. Incident Response Training
Authority- DIR CC: IR-2

a. ASU must provide training annually to all users on their responsibilities in reporting issues with technology.

b. ASU must train employees to involve information security personnel in any suspected information security incidents.

c. The Office of Information Technology will provide annual training to personnel with incident response roles and responsibilities.

4. Incident Handling
Authority-DIR CC: IR-4

a. ASU must implement an incident handling capability that includes preparation, detection and analysis, containment, eradication, and recovery and adapts to create effective resolutions.

b. ASU must coordinate incident handling activities with contingency planning activities.

5. Incident Monitoring
Authority-DIR CC: IR-5

a. ASU must track and document security incidents.

b. Information security personnel must track and ensure security incidents are well documented.

c. Information security personnel must store documentation of security incidents in a secure fashion.

6. Incident Reporting
Authority-Texas Administrative Code: 202.73(b), DIR CC: IR-6

a. ASU requires users promptly report security incidents to the Office of Information Technology.

b. Incidents involving information security must be reported to and managed by the ISO and will be promptly reported as required by federal or state law or regulation.

c. Incidents that require prompt reporting to DIR include those that may:

(1) Propagate to other state systems;

(2) Result in criminal violations that shall be reported to law enforcement; or

(3) Involve the unauthorized disclosure or modification of confidential information.

d. ASU must report summary security incident information monthly to DIR within 9 days after the end of the month.

e. In the event a complete report of a security incident cannot be submitted at once, ASU will report circumstances of the incident as they are discovered.

f. ASU must disclose breaches of sensitive information in accordance with all applicable law unless the university receives a request from law enforcement to delay disclosure to prevent impact to an active investigation.

g. ASU must provide means and methods for users to report security incidents that allow for immediate and effective communication to information security personnel.

h. If ASU suspects an incident may involve criminal activity, ASU must immediately turn over all pertinent incident information to appropriate law enforcement authorities and restore to operation promptly while meeting the legal requirements for handling evidence.

i. ASU must ensure vendor security incident reporting requirements are included in contracts.

7. Incident Response Assistance
Authority-DIR CC: IR-7

a. The incident management team reviews all incidents to assess any potential security impact.

b. The incident management team must notify the ISO of any potential security incidents.

c. The incident management team resolves the incident in consultation with the ISO.

d. The ISO must provide advice and assistance to users of the information system for the handling of security incidents.

8. Incident Response Plan
Authority-DIR CC: IR-8

a. ASU must create and distribute a security incident response plan that:

(1) Outlines incident response;

(2) Describes the requirements for dealing with security incidents including prevention, detection, response, and remediation;

(3) Ensures incident response meets university needs;

(4) Defines which incidents must be reported and handled as security incidents;

(5) Defines metrics to monitor effectiveness; and

(6) Defines support needed to maintain and mature incident response.

b. ASU must distribute, update, communicate and protect the incident response plan as necessary.