[New policy: January 5, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.12: Personnel Security

DATE: January 5, 2018

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

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. Personnel Security Policy and Procedures
Authority-DIR Controls Catalog (CC): PS-1

a. ASU must establish a personnel security policy (see OP 52.55 and OP 52.56).

b. ASU must ensure personnel follow university policy, taking disciplinary action as needed.

3. Position Risk Designation
Authority- DIR CC: PS-2

a. ASU must identify security sensitive positions (to include all Office of Information Technology positions) and ensure sensitive information handling responsibilities are included in position descriptions.

b. ASU must apply screening criteria for individuals being hired for security sensitive positions.

c. All authorized users of information systems must acknowledge that they will comply with the security policies and procedures of the university (see OP 44.00 and OP 44.14).

4. Personnel Screening
Authority-DIR CC: PS-3

a. ASU must screen employees prior to being authorized to access information systems.

b. Per OP 52.56, ASU requires employees to report arrests, convictions, or judgements to their supervisor within 24 hours or at the earliest possible opportunity thereafter.

5. Personnel Termination
Authority-DIR CC: PS-4

a. ASU must disable access to information systems for terminated employees within a reasonable period.

b. ASU must retrieve university owned credentials, keys, and information system hardware from the terminated employee.

c. ASU must notify appropriate individuals of employee termination.

d. Upon request of a terminated employee's department chair and in coordination with the ISO, the custodian must provide authorized university employees access to records created by the terminated employee that are stored on university information systems.

6. Personnel Transfer
Authority-DIR CC: PS-5

a. ASU must notify custodians of terminations and transfers.

b. Upon notification of terminations and transfers, custodians must modify access as required.

7. Access Agreements
Authority-DIR CC: PS-6

a. ASU requires employees to sign a written agreement to follow university policies prior to accessing university information and information systems.

b. ASU must require employees sign a FERPA release statement prior to accessing information systems containing FERPA information.

c. ASU requires employees to sign an access agreement before provisioning access to ERP systems.

d. Employees must not use university information systems for political lobbying or campaigning.

8. Third-Party Personnel Security
Authority-DIR CC: PS-7

a. Third-party access to information systems must be time-limited.

b. Organizations affiliated with the university must abide by the law and university policy.

c. Third-party vendors must abide by the law and university policy.

d. ASU must monitor third-party compliance.

[New policy: January 5, 2018]

9. Personnel Sanctions

Authority-DIR CC: PS-8

a. ASU must maintain a formal disciplinary process for individuals failing to comply with university policy (see OP 52.10).