[New policy: January 5, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.08: **Identification and Authentication**

DATE: January 5, 2018

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

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. Identification and Authentication Policy and Procedures

Authority-DIR Controls Catalog (CC): IA-1

a. ASU must verify the identity of a user, process, or device, before granting access to resources in an information system.

b. ASU must use identification and authentication of users, processes or devices to protect information systems based on risk posture.

c. ASU must keep identification and authentication procedures current.

3. Identification and Authentication (Organizational Users)

Authority- DIR CC: IA-2

a. ASU must assign a unique identifier to each user, or process acting on behalf of a user, that will identify the account through the entire lifecycle of the identity based on system risk posture.

b. ASU must authenticate users before allowing access to university information.

4. Identifier Management

Authority-DIR CC: IA-4

a. ASU must change user access when a user's role within the university changes. Human Resources must provide notification of role changes to custodians.

b. ASU assigns identities to users permanently without identity reuse.

c. Information owners must authorize the assignment of identities.

5. Authenticator Management

Authority-DIR CC: IA-5

Credential Establishment

a. ASU must create all accounts using a uniquely identifiable username assigned by the Office of Information Technology or information owner.

b. All accounts must be associated with an identifiable individual or group of individuals authorized to use the account.

c. Each user must be associated with a single unique identity within the authentication realm.

d. All user accounts must meet the same requirements, to include all vendor, consultant, and contractor accounts.

e. Information owners must authorize all accounts prior to use.

Account Controls

f. Where supported by the underlying accounting mechanism, all user accounts must have a password expiration appropriate to the risk posture of the system. Service accounts may be exempted from this requirement based on a current risk assessment of the system and supported application/service.

g. Authentication credentials must meet the following minimums:

(1) All account passwords must comply with the following minimum password complexity requirements:

(a) Must be at least eight (8) characters in length; and

(b) Must be changed no less often than every 120 days.

(2) Account passwords associated with sensitive information must also comply with the following minimum password complexity requirements:

(a) Contain a mixture of uppercase and lowercase letters, numerals, and special characters;

(b) NOT re-use any of the account’s last 24 passwords; and

(c) NOT include personal information such as your name and account name.

(3) The ISO must approve exceptions to minimum password quality requirements.

h. Password changes must comply with password strength requirements associated with the classification of the service in question, where supported by the underlying accounting mechanism.

i. ASU must encrypt authentication credentials where possible.

Account Handling Procedures (for issuance, loss, damage, or revocation)

j. Accounts of individuals, who have had their status, roles, or affiliations with the university change or who have become separated from the university, must be updated/ revoked to reflect changes to their status in a timely manner.

k. ASU must review accounts to ensure their status is correct on a schedule consistent with risk posture of the system.

l. University identity credentials (smart cards, security tokens, and other access/id devices) must be disabled or returned to the appropriate person on demand or upon termination of the relationship with the university.

m. ASU must disseminate account information securely to authorized users.

n. User's identity must be vetted when issuing an account or resetting a password.

o. Custodians must implement control procedures to limit impact of account compromise.

p. Individuals issued authentication credentials must keep the credentials (including username, password, keycard and tokens) confidential, report any suspected loss or exposure to the Office of Information Technology, and not share credentials.

q. ASU must change factory-preset accounts to meet university requirements prior to putting the system into production.

6. Authenticator Feedback

Authority-DIR CC: IA-6

a. Where possible, ASU must mask password entry.

b. Where possible, login failures must not indicate which part of the username/password combination is incorrect.

7. Cryptographic Module Authentication

Authority-DIR CC: IA-7

a. ASU must follow all applicable laws and regulation regarding the use of cryptographic modules and encryption.

8. Identification and Authentication (Non-Organizational Users)

Authority-DIR CC: IA-8

a. Access to information systems by non-organizational users requires approval by the information owner.

b. ASU must configure information systems to authenticate and uniquely identify non-organizational users.

c. ASU must configure public systems only to allow access to information that is appropriate for public consumption.