[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.02: Access Control

DATE: June 21, 2018

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

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. Access Control Policy and Procedures
Authority-DIR Controls Catalog (CC): AC-1

a. ASU must establish and implement account management policy elements to ensure secure user access to university information using controls such as approvals, time limits on access, regular authorization reviews, role-based access control, and unique user identifiers.

b. ASU must grant access based on user's current role(s).

c. Information owners must approve all access directly or through pre-approved processes.

d. Monitoring user access to information systems is established and defined in OP 44.04.

3. Account Management
Authority- DIR CC: AC-2

a. ASU must establish user access to information systems using system accounts.

b. ASU must ensure confidential information is accessible only to authorized users. All access requests for access to information systems containing confidential information (Category 1, 1a or 2) must follow an account creation process that includes appropriate approvals from the information owner. Requirements for protecting confidential information are established and defined in OP 44.20.

c. All accounts must be uniquely identifiable using a centrally assigned user name from the Office of Information Technology or information owner. ASU defines user identity and establishes user identification policy in OP 44.08.

d. ASU must associate all accounts with an identifiable individual or a group of individuals (with compensating controls approved by the ISO) who are authorized to use the account.

e. Access to information systems must match role and/or have approval from the information owner.

f. ASU must update/revoke accounts of individuals, who have had their status, roles, or affiliations with the university change or who have become separated from the university, to reflect changes to their status in a timely manner.

g. Accounts must be reviewed at least annually to ensure their status is correct.

h. Where supported by the underlying accounting mechanism, all user accounts must have a password expiration that complies with the university password policy. ASU may exempt service accounts from this requirement based on a current risk assessment of the system and supported application/service.

i. Information systems must have access controls based on documented university risk management decisions.

j. All vendor, consultant, and contractor accounts must comply with all requirements of this section.

4. Access Enforcement
Authority-DIR CC: AC-3

Access to information systems must be managed using the following:

a. All systems with information not entirely classified as Category 3 (public information) must use authentication.

b. All systems using authentication must require users to use unique, individually assigned credentials. Shared accounts must be assigned to a primarily responsible individual and issuance requires the approval of the ISO.

c. Access to information is controlled through centralized authentication where possible and overseen by both custodians and information owners to ensure only authorized individuals are allowed access to university managed information.

d. Users must request access through the custodian's ticketing system or by following access control procedures.

e. ASU information systems must authenticate user credentials prior to allowing access to the information system or university data.

f. Where possible, systems must authenticate end user passwords against identified centralized systems in this preference order:

(1) Single sign-on

(2) Authentication against centralized systems

(3) Synchronized account names and passwords from centralized systems

(4) Local system account name and password

g. Custodians must not bypass access controls in production systems except under safe conditions and approval by the ISO.

5. Separation of Duties
Authority-DIR CC: AC-5

a. Information owners are required to consider separation of duties when approving access within systems such as separation of duties between programmers and developers.

b. Custodians must ensure access control enforces separation of duties when setting up information system access.

c. ASU must use adequate controls to provide separation of duties for tasks that are susceptible to fraud or other unauthorized activity.

6. Least Privilege
Authority-DIR CC: AC-6

Anyone using accounts with elevated privileges must adhere to the following requirements:

a. Individuals who use administrative accounts with elevated privileges must use these accounts only for their intended administrative purposes.

b. ASU must maintain records of all users who have access to administrative account credentials.

c. Password expiration is not required on shared administrator accounts.

d. The password for a shared administrator account must change when any individual knowing the password no longer should have access (e.g., terminated university employee, change in support vendor staff, or changes in university employee role).

e. A password escrow must be in place for all administrative accounts to enable someone other than the custodian to gain access to the system in an emergency.

f. When using elevated privileges for auditing, software development, software installation, or other defined needs, they must:

(1) Receive authorization from the information owner;

(2) Have an expiration date where supported; and

(3) Be removed when work is complete.

g. Prior to permitting users access to university information, ASU must ensure the duties assigned to users require access to university information.

7. Unsuccessful Logon Attempts
Authority-DIR CC: AC-7

a. Access control systems must limit unauthorized logons on centralized authentication systems by putting a lockout on accounts after at most ten (10) failed logon attempts. As technology permits, systems not using centralized authentication will have lockout settings appropriate to risk posture of the system.

b. Centralized authentication systems must use timed lockout of at least 30 minutes. As technology permits, systems not using centralized authentication will have timed lockout settings appropriate to risk posture of the system.

8. System Use Notification
Authority-DIR CC: AC-8

a. ASU information systems should, where appropriate based on risk management assessments, display an approved system use notification message before granting access to the system.

b. The logon banner should cover the following topics:

(1) Unauthorized use is prohibited;

(2) Usage may be subject to security testing and monitoring;

(3) Misuse is subject to criminal prosecution; and

(4) Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

c. Information systems containing only Category 3 information, and intended for public use, does not require an approved system use notification message unless required by the information system's risk posture.

9. Permitted Actions Without Identification or Authentication
Authority-DIR CC: AC-14

a. ASU must use appropriate access controls to protect the integrity and availability of Category 3 information.

b. ASU requires identification and authentication on all information systems including those containing only Category 3 information. Some uses of information systems may be exempted to not require authentication such as general form submission and anonymous fraud reporting.

c. Any actions that may be performed on an information system require identification or authentication except in the event of an emergency.

10. Remote Access

Authority-DIR CC: AC-17

a. Remote access to the university network must use university-approved methods.

b. ASU requires the same policies for authentication and authorization for local and remote access. The ISO may require additional authentication or approvals for remote access.

c. The Office of Information Technology must document and regularly review usage restrictions, configuration and connection requirements, and implementation guidance for all types of remote access allowed.

d. The Office of Information Technology must approve access to remote access technologies (including VPN) prior to connection.

e. The Office of Information Technology must validate user access to remote access technologies (including VPN) annually.

f. Remote access must authenticate through Office of Information Technology approved authentication mechanisms configured within the remote access termination point.

11. Wireless Access

Authority-DIR CC: AC-18

a. All wireless connections to university information systems must comply with Office of Information Technology requirements.

b. Wireless networks must use industry and vendor recommendations for securing wireless networks including changing factory-installed settings (see OP 44.06) and using appropriate encryption technologies such as VPN/WPA.

c. Only personnel authorized by the Office of Information Technology may configure wireless networks.

d. Users must not install or configure wireless networks, ad hoc or otherwise, unless specifically authorized by the CIO in writing.

e. The Office of Information Technology must prohibit and monitor for unauthorized wireless networks.

f. ASU requires authentication and encryption be used for transmitting sensitive information over wireless networks.

g. A public access network is available for incidental use by campus visitors. ASU must use appropriate security controls to separate public access networks from secure networks.

h. Public (open) wireless networks must require agreement to acceptable use policy before allowing connections.

12. Access Control for Mobile Devices

Authority-DIR CC: AC-19

a. Information security policies govern all devices used to store, transmit, or process university information whether university or personally owned and include, but are not limited to: tablets, smartphones, desktop computers and laptops.

b. All university or personally owned devices used to store or process university information must use a method to control access to the device as follows:

(1) University or personally owned devices that store or process Category 1 information must use a complex password containing at least three of the following: uppercase letters, lowercase letters, numerals, punctuation.

(2) University or personally owned devices that store or process Category 1a or 2 information must use at a minimum a PIN, gesture lock, biometrics or password to access the device.

c. Category 1 information stored or processed directly on university or personally owned devices or removable media must be encrypted. Category 1a or 2 information stored or processed directly on university or personally owned devices or removable media should be encrypted or use other compensating controls to protect the confidentiality and integrity of the information.

d. Category 1 or 1a information transmitted to/from university or personally owned devices must use encryption.

e. University or personally owned devices used to store or process Category 1 or 1a information should be kept in the owner's direct possession or be otherwise physically secured using reasonable means. Any university or personally owned device used to store or process Category 1 or 1a information should not be left unattended in public places or automobiles.

f. Users must immediately report loss or theft of any devices used to store or process Category 1 or 1a information to the Office of Information Technology.

g. Devices must use university approved methods and configurations in accordance with all university policies when connected to university networks.

h. Devices must use authentication systems managed by the Office of Information Technology when connecting to campus networks.

i. ASU must monitor device use of university networks.

j. The Office of Information Technology must provide secure device configuration information that includes usage restrictions, configuration requirements, connection requirements, and implementation guidance.

13. Use of External Information Systems
Authority-DIR CC: AC-20

a. ASU must use established terms and conditions for contracts to protect the confidentiality, integrity and availability of university information systems managed by or connected to by third parties.

b. University must establish rules requiring vendors and contractors to provide similar, if not equal, controls required to protect the university's information and systems.

c. All categories of university information may be stored on non-university information systems as long as the information is verifiably protected according to the respective university minimum security standards and approved by the information owner and ISO (see data classification standard for more information).

14. Publicly Accessible Content
Authority-DIR CC: AC-22

a. ASU trains personnel in protecting the confidentiality of Category 1 and 1a information.

b. ASU must establish procedures to ensure the integrity of the information posted publicly on university information systems.

c. ASU designates and trains personnel authorized to post information publicly.

d. Authorized personnel must ensure sensitive information is not posted publicly.