Angelo State University
Operating Policy and Procedure

OP 44.00: Information Technology Operating and Security Policy

DATE: September 17, 2014

PURPOSE: The purpose of this policy is to define Office of Information Technology operating policies for the management and security of information resources.

REVIEW: This OP will be reviewed in July every three 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. Overview

ASU information resources are provided to support the instructional, research, public service, and administrative objectives of the university. Angelo State University policies, Texas Tech University System regulations, and state and federal law govern the use of information resources. The information resources infrastructure is provided for the entire campus. This infrastructure is finite and is expected to be used responsibly and with courtesy, respect, and integrity.

2. Reference

Further clarification or implementation guidance concerning this policy may be found on the information security website.

3. Definition

For terms referred to in this document but not defined in this section refer to the information technology glossary.

a. Information resource - any data or system such as files, computers, tablets, servers, hard drives, removable thumb drives, etc.

b. Category I information - the most sensitive information used at the university and covers items protected by law. For more information refer to data classification standard.

c. Category II information - information not normally released to the public unless through a legal information request such as a subpoena or Freedom of Information Act request. For more information refer to data classification standard.
d. Backup - copy information to another location to prevent loss.

e. Use - an umbrella term that includes, for purposes of this document, the terms store, process, change, delete, read, and access.

f. Hardening - the process of making computer and network systems more resistant to tampering or malicious software.

g. Patch - a fix or update for a software program usually related to a security issue.

h. Production system - a computer system used to directly support university operations and not used exclusively for testing or software development.

i. Test and development systems - systems used exclusively for testing or development of software and not used to directly support university operations.

j. Anti-malware software - a program or programs built to prevent malware (malicious software) from affecting computer software and hardware. This is a term that includes anti-virus software.

k. Penetration test - a controlled attempt to circumvent the security of a network or computer system to test its ability to resist hacking.

4. Acceptable Use

   Authority-Texas Administrative Code (TAC): 202.75.7.A; 202.75.7.G

   a. Users are required to report any weaknesses in security controls, incidents of misuse, and violations of university information technology operating and security policies to the Information Security Office.

   b. Users will not attempt to access, change, or delete any data or programs contained on university information resources for which they do not have authorization or explicit consent to do so.

   c. Users must not share their university account(s), passwords, PINs, hardware/software tokens, or similar devices (such as smartcards) used for authentication and authorization purposes.

   d. Users are responsible for all actions that take place with their university account(s), passwords, PINs, hardware/software tokens, or similar devices (such as smartcards) used for authentication and authorization purposes. Users who share their access with another individual will be held responsible for all usage of their access.

   e. Users are responsible for all actions that take place with personally owned devices when using university information or connecting to university information resources.

   f. Users must not engage in unauthorized reproduction or distribution of intellectual property protected under copyright, trademark or patent law.

   g. Users must not purposely engage in activity that may harass, threaten, intimidate, endanger, or abuse others; degrade the performance of information resources; deprive an
authorized user access to a university resource; obtain resources beyond those allocated; or circumvent university technology security measures.

h. Users must not download, install, or run security programs or utilities that reveal or exploit weaknesses in security controls of university systems without explicit approval from the Information Security Office.

i. Users must not use university information resources for political lobbying or campaigning.

j. Users must not use or disclose protected information, or data that is otherwise confidential or restricted, without appropriate authorization. Refer to OP 44.01 for further detail.

k. As a convenience to the university community, limited incidental use of information resources is permitted. Incidental use must:

(1) Not result in any burden or direct cost to the university; and

(2) Not interfere with the normal performance of an employee’s work duties; and

(3) Not include sending or receiving files or documents that may cause legal action against, or embarrassment to, any Texas Tech University System institution; and

(4) Make available all personal email, voicemail, files, and data located on university information resources to applicable open records requests (such requests must follow the university standard formal request process).

5. **Account Management**  
   **Authority-TAC: 202.75.7.B**

a. All access requests for category I or II information resources must follow an account creation process that includes appropriate approvals.

b. All accounts must be uniquely identifiable using a centrally assigned user name from the Office of Information Technology or information owner.

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

d. 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.

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

f. Where supported by the underlying accounting mechanism, all user accounts must have a password expiration that complies with the university password policy. Service accounts may be exempted from this requirement based on a current risk assessment of the system and supported application/service.
g. Information resources must have access controls that are based on documented university risk management decisions.

h. All vendor, consultant, and contractor accounts must comply with all requirements in this section.

6. Administrative Accounts
Authority-TAC: 202.71, 202.75.7.C

Anyone using accounts with elevated privileges (including "special access" accounts per TAC 202.75.7.C) 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. Records must be maintained 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 situation.

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

   (1) Must be authorized by the information owner or custodian;

   (2) Must be created with an expiration date when supported;

   (3) Must be removed and disabled when work is complete.

g. Investigations of misuse of an information resource must be performed only under the direction of the Information Security Office and/or the CIO.

7. Backup and Business Continuity
Authority-TAC: 202.75.7.E, 202.74

The frequency and content of backups will balance risk tolerance and cost determined by risk assessment.

a. The vendor(s) providing offsite backup storage for the university must be approved to handle the highest level of information stored.

b. Physical access controls implemented at offsite backup locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest university sensitivity level of information stored.
c. A process must be implemented to verify the success of the university electronic information backup.

d. Backups must be periodically tested to ensure they are recoverable.

e. Procedures between the university and the offsite backup vendor(s) must be reviewed at least annually.

f. Only university approved storage or services may be used to store or backup category I information.

8. **Change Management**

   **Authority-TAC: 202.75.7.F**

   Changes must comply with the following:

   a. Review by technical assignee’s management prior to implementation.

   b. Review by information owner representative prior to implementation.

   c. Provide prior communication of any scheduled outages.

   d. Document proper back out and recovery procedures.

   e. Log appropriate information for all changes.

   f. Conduct weekly reviews to evaluate and coordinate proposed changes.

9. **Security Incident Management**

   **Authority-TAC: 202.75.7.J; 202.76**

   a. Incidents involving computer security must be managed by the Information Security Office and will be reported as required by federal or state law or regulation (including Texas Department of Information Resources' requirements for security incident reporting). All security incidents will be resolved as quickly as possible while meeting the legal requirements for handling evidence and taking into consideration:

      (1) The time necessary to determine the scope of the incident and restore the reasonable integrity of operations; and

      (2) Any request of a law enforcement agency to prevent interfering with a criminal investigation. If so, resolution must be made as soon as the law enforcement agency notifies the Information Security Office of its determination that the resolution will not compromise the law enforcement investigation.

   b. If pertinent to an information security investigation, users may be asked to provide access to personally owned devices used to store or process university information. If permission is not given, the user's access to university information resources may be terminated.
10. Network Access

Authority-TAC: 202.75.7.N, 202.75.7.Z, 202.77.a

All users are required to maintain a high level of security and performance for the services on the university network by:

a. Accessing services in accordance with their deployed purpose using proper account credentials when required.

b. Using only network addresses provided by the Office of Information Technology.

c. Using only those remote access services provided by the Office of Information Technology.

d. Removing connections to external networks before connecting to the university network.

e. Not extending or retransmitting network services in any way.

f. Not altering network hardware or software in any way.

g. Not configuring ad hoc wireless networks.

h. Configuring all non-university owned systems to meet networking standards.

11. Network Configuration

Authority-TAC: 202.75.7.1, 202.75.7.O, 202.75.7.W, 202.75.7.Z

The Office of Information Technology and its approved subcontractors are the only authorized personnel to perform the following:

a. Design, deploy, and support all network infrastructure and wiring for the university.

b. Install all communications cabling.

c. Approve and implement configuration changes to network infrastructure.

d. Alter network hardware and cabling.

e. Extend network hardware and software.

f. Establish and manage all protocols used on the university network.

g. Allocate and distribute network addresses.

h. Establish and manage connections to third party data and networks.

i. Install and configure all network firewalls.

(1) Manage virtual and physical architecture.

(2) Manage protocols and applications permitted through the firewall.
(3) Manage traffic monitoring rule sets.
(4) Monitor and enforce the firewall policy.
(5) Update rule sets with approval.
(6) Audit and test firewall configuration, rule set accuracy and effectiveness.

j. Configure and control all wireless signals providing access to the university network.
k. Create and maintain all university network infrastructure standards and guidelines.

12. Passwords
   Authority-TAC: 202.75.7.K

   a. Password Quality

      (1) All account passwords must comply with the following minimum password complexity requirements:
          (a) Must be at least 8 characters in length;
          (b) Must be changed no less often than every 120 days.

      (2) Account passwords associated with protected information must also comply with the following minimum password complexity requirements:
          (a) Contain a mixture of uppercase and lowercase letters, numerals, and special characters; and
          (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) Exceptions to minimum password quality requirements must be approved by the Information Security Office.

   b. End User Accounts

      (1) Where possible, systems must authenticate end user passwords against identified centralized systems in this preference order:
          (a) Single sign-on
          (b) Authentication against centralized systems
          (c) Synchronized account names and passwords from centralized systems
          (d) Local system account name and password

      (2) User’s identity must be vetted when issuing an account or resetting a password.

      (3) Password changes must comply with password strength requirements associated with the data classification of the service in question, where supported by the underlying accounting mechanism.
c. 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.

13. Physical Access  
Authority-TAC: 202.75.7.P; 202.73

a. All physical security systems must comply with all applicable regulations such as, but not limited to, building and fire safety codes.

b. All information resources must be physically protected in proportion to the criticality or importance of their function.

c. The process for granting card and/or key access to information resource facilities must include the approval of the person responsible for the facility.

d. Access cards and/or keys must not be shared or loaned to others.

e. Access cards and/or keys that are no longer required by the person to whom they were assigned must be returned to the appropriate university department.

f. Lost or stolen access cards and/or keys must be reported immediately to one’s supervisor or the Information Security Office.

g. A service charge may be assessed for access cards and/or keys that are lost, stolen, or are not returned.

h. Card access records and visitor logs for information resources facilities must be retained and reviewed regularly.

i. The card and/or key access rights of individuals who change roles or are separated from their relationship with the university must be removed.

j. Where applicable, alarm codes will be assigned to staff and approved vendors as determined necessary by the person responsible for the facility.

k. Alarm codes must not be shared or loaned to unauthorized users.

l. All institutional operating policies are applicable to university equipment used off site.

m. Physical security procedures for information resource facilities must be reviewed at least annually.

n. The State Office of Risk Management will be referred to for applicable rules and guidelines.

Items o – r are applicable to information resource facilities designated as non-public restricted access facilities:

o. Access to information resource facilities must be granted only to university support personnel, and approved contractors, whose job responsibilities require access to the facility.
p. Visitor access to information resource facilities must be tracked with a sign in/out log.

q. Visitors accessing information resource facilities must be escorted.

r. Information resources must be protected from environmental hazards. Designated employees will be trained to monitor environmental control procedures and equipment and must be trained in desired response in case of emergencies or equipment problems.

Items s - t are applicable to information resource facilities designated as computer labs:

s. Protected information must not be stored on computing hardware in information resource facilities defined as computer labs.

t. Access to computing equipment in information resource facilities defined as computer labs must be approved by facility owner.

14. Mobile Devices

Authority-TAC: 202.75, 202.77, 202.78(b)(2)

a. All devices used to store, transmit, or process university information whether university or personally owned are governed by this policy and include, but are not limited to: tablets, smart phones, 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 I 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 II information should use a PIN, gesture lock, or password to access the mobile device.

c. Category I information stored or processed directly on university or personally owned devices or removable media must be encrypted. Category II information stored or processed directly on university or personally owned devices or removable media should be encrypted or use other compensating controls.

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

e. University or personally owned devices used to store or process category I or II 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 I or II information should not be left unattended in public places or in automobiles.
f. Loss or theft of any devices used to store or process category I or II information must be reported to the Technology Service Center immediately.

g. Devices used to connect to university information resources should be managed, configured, and used in accordance with all university policies and law.

15. Privacy of Electronic Information  
Authority-TAC: 202.75.7.R

a. Electronic files and data created, sent, received, stored, or transmitted across computers or other information resources owned, leased, administered, or otherwise under the custody and control of the university are not private unless expressly stated in federal or state law; however, applicable open records requests must follow the university standard formal request process. (Refer to OP 01.02.)

b. The university may log, review, capture, and otherwise use information stored on or passing through its information resources as needed for the purpose of system administration and maintenance, for resolution of technical problems, for compliance with Texas Public Information Act, for compliance with federal or state subpoenas, court orders, or other written authorities, to conduct the business of the university, for resolution of information security incidents and to perform audits. No notification is required to view this information; however, users with privileged access are expected to maintain the privacy of the individual where permissible by law.

c. Identifying information must be removed before sharing collected information to prevent loss of individual privacy where possible.

d. Employees, contractors, vendors, and affiliates of the university must safeguard the privacy and security of any information owned by or entrusted to the university.

16. Security Monitoring  
Authority-TAC: 202.75.7.S

a. To ensure compliance with these policies, state laws and regulations related to the use and security of information resources, the university’s Information Security Office has the authority and responsibility to monitor information resources to confirm that security practices and controls are adhered to and are effective.

b. If the operating system or application software comes with means to log activity, controls enabled must be consistent with system risk. All controls used should be tested before being implemented for general use.

c. Routine monitoring and analysis of operating system and application logs are required on a schedule consistent with system risk.

d. Backup strategies for security logs should be consistent with security risk.

e. Logging of administrator and root access should be consistent with security risk.

f. Any security issues discovered during log review or alerting must be reported to the Information Security Office for follow-up investigation.
17. Security Awareness and Training  
Authority-TAC: 202.75.7.T; 202.77.a; 202.77.d-e  

a. All users, including students and employees, must acknowledge that they have read, understand, and will abide by university information security policies when granted access to information resources.

b. Security awareness programs and/or materials must be provided at least annually to employees and students.

c. The Information Security Office must develop required technical training for employees providing support of information resources.

18. System Hardening  

a. A system must not be connected to the university network until assessed as securely configured and approved by the Office of Information Technology. Vendor configurations must be overwritten with university approved configurations.

b. The degree of hardening for applications must be in accordance with the value of the information and the acceptable risk as determined by the information owner.

c. Security issues, internal and external to the university, must be monitored.

d. Security patches must be tested by the Office of Information Technology before release into production where practical.

e. Where practical, resources must be made available for testing security patches.

f. Security patches must be applied within a timeframe specified by the Office of Information Technology.

g. Appropriate login banners must be placed at connection points to systems to identify that access is allowed only in accordance with this document and TAC 202.75.9.

h. Systems designated for public access must be configured to enforce security policies and procedures without the requirement for formal acknowledgement.

19. Software Licensing and Copyright  
Authority-TAC: 202.75.7.V  

a. Copies of software licensed by the university must be made only in accordance with the license agreement.

b. Software used on university owned systems must be properly licensed for its method of use (concurrent licensing, site licensing, or per system licensing).

c. The university must remove inappropriately licensed software from university owned systems.
20. System Development and Acquisition

Authority-TAC: 202.75.7.W; 202.75.6 (A-C)

a. Mission critical software implementations must use the Information Technology Project Office standard to address a preliminary analysis, risk identification, university goal alignment, planned timeframe, scope, and budget. Non-mission critical software implementations should follow this process as closely as possible.

b. All production systems must have designated information owners and custodians.

c. Where resources permit, separation between the production, development, and test environments will exist. Development and test environments containing production data must use the same security protections as production systems.

d. Patches and upgrades should be evaluated in a test environment, when available, prior to being installed in a production environment.

e. Critical patches must be applied on a regular basis and non-critical patches should be applied as needed.

f. Changes or upgrades to a production system must follow a standard methodology.

21. Vendor Access

Authority-TAC: 202.75.7.X

a. Vendors must comply with all applicable university policies and agreements.

b. Vendor agreements and contracts must specify:

   (1) The university information resources to which the vendor should have access.

   (2) How university data is to be protected by the vendor.

   (3) Acceptable methods for the return, destruction, or disposal of university data in the vendor’s possession at the end of the contract.

   (4) The vendor must use university data and information resources only for the explicitly granted purposes of the business agreement.

   (5) Any other university data acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes, or divulged or transferred to others.

c. Each vendor with access to protected information owned by the university must be approved to handle that information.

d. If a vendor is involved in university security incident management, the responsibilities of the vendor must be specified in the contract.

e. Vendors must observe regular work hours and duties as requested. Work outside of defined parameters must be approved by appropriate university personnel.
22. Affiliated Organizations  
   Authority: University Policy (OP 14.13)  

   Affiliated organizations must abide by the provisions and requirements of this policy along with the university operating policy. (Refer to OP 14.13).

23. Malicious Code  
   Authority: TAC: 202.75.7.Y  

   All devices, whether personally or university owned, used to store or process category I university information are required to:  
   a. Use Office of Information Technology approved anti-malware software and a university approved secure configuration.  
   b. Prevent disabling or bypassing anti-malware software.  
   c. Prevent any changes to anti-malware software that will reduce the effectiveness of the software.  
   d. Be configured to update anti-malware software at least monthly.  
   e. Report any malware detected but not cleaned or quarantined. Users should notify the Technology Service Center of this malware.

24. Vulnerability Assessment  
   Authority: TAC: 202.75.7.AA  

   a. Annual controlled penetration tests by an external entity must be performed.  
   b. Ad hoc vulnerability assessments should be performed as relevant vulnerabilities are published that may affect the security profile of an information resource.

25. Risk Management  
   Authority: TAC: 202.71, 202.72, 202.75.2  

   a. Under the guidance of the Information Security Office, the university must conduct and document an information security risk assessment according to state regulatory guidelines. Angelo State University will rank inherent risk as high, medium, or low and perform biennial assessments for medium and low risks and annual for high risks.  
   b. The confidentiality, integrity, and availability of information resources must be managed and protected based on sensitivity and risk. Selection and application of controls will balance cost against the risk and sensitivity of the university information.

26. Data Classification and Risk Assessment  
   Authority: TAC: 202.71, 202.72, 202.75.2  

   a. Information owners or designated custodians are required to classify information resources under their purview using a balanced approach based on sensitivity of the data and cost of controls to protect it.  
   b. The data classification standard must be used to identify digital data that is sensitive.
c. Information resources may be classified at a higher level if warranted by a school or department’s demonstrated need.

d. With written justification of a demonstrable business need, the university may move an information resource to a lesser classification upon request by the information owner, after appropriate review and approval by the Information Security Office.

27. Disciplinary Action

Violation of this policy may result in disciplinary action leading to or including termination for employees; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of access to Angelo State University information resources, and civil or criminal prosecution.