



**Angelo State University**  
**Operating Policy and Procedure**

**OP 44.00: Information Technology Operating and Security Policy/Procedures**

**DATE:** March 4, 2011

**PURPOSE:** The purpose of this Operating Policy/Procedure is to define Information Technology Operating Policies for the management and security of Information Resources.

**REVIEW:** This Operating Policy (OP) will be reviewed in December of every year by the Information Security Officer and appropriate personnel with recommended revisions forwarded through the Information Technology CIO and vice presidents to the president by January 15 of the next year.

**AUTHORITY:** The contents of the Policy/Procedures listed below ensure the university's compliance with Texas Administrative Code (TAC) 202.

**DEFINITION:** Reference associated document located on Information Technology website: [http://www.angelo.edu/services/technology/it\\_policies/glossary.html](http://www.angelo.edu/services/technology/it_policies/glossary.html)

**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.

**POLICY/PROCEDURE**

**1. Acceptable Use**

**Authority – TAC: 202.75.7.A; 202.75.7.F; 202.75.7.H**

- a. Users shall 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 shall not attempt to access any data or programs contained on university information resources for which they do not have authorization or explicit consent to do so.
- c. Users shall not share their university account(s), passwords, PINs, 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, 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 shall not engage in unauthorized reproduction or distribution of intellectual property protected under copyright, trademark or patent law.
- f. Users shall not purposely engage in activity that may: harass, threaten, 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.
- g. Users shall 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.
- h. Users shall not use university information resources for political lobbying or campaigning.
- i. Users shall not use or disclose Category-I data, or data that is otherwise confidential or restricted, without appropriate authorization.
- j. As a convenience to the university community, limited incidental use of information resources is permitted. Incidental use shall:
  - (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 shall follow the university standard formal request process).

## **2. Account Management**

### **Authority-TAC: 202.75.7.B**

- a. All access requests for Category-I/-II information resources shall follow an account creation process that includes appropriate approvals.
- b. All accounts shall be uniquely identifiable using a centrally assigned user name from the Information Technology department.
- c. All accounts shall be associated with an identifiable individual or group of individuals that 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, shall be updated/revoked to reflect changes to their status in a timely manner.

- e. Accounts shall be reviewed to ensure their current status is correct at least annually.
- f. Where supported by the underlying accounting mechanism, all user accounts shall have a password expiration that complies with the university password policy.
- g. All vendor, consultant, and contractor accounts shall follow these measures.
- h. Information resources shall have access controls that are based on documented university risk management decisions.

### **3. Administrative/Special Access Accounts**

**Authority-TAC 202.75.7.C**

Users shall be aware of the privileges granted to administrative/special access accounts. Abuse of such privilege is not tolerated. Anyone using accounts with elevated privileges shall adhere to the following requirements:

- a. Individuals who use administrative/special access accounts with special privileges shall use these accounts only for their intended administrative purposes.
- b. Records shall be maintained of all users who have access to administrative/special access account credentials.
- c. The password for a shared administrator/special access account shall follow the password policy guidelines.
- d. The password for a shared administrator/special access account shall change when any individual knowing the password leaves the university or changes roles and no longer should have access to the password; or upon a change in the vendor personnel assigned to university contracts having password access.
- e. A password escrow shall be in place for all administrative/special access accounts to enable someone other than the Custodian to gain access to the system in an emergency situation.
- f. When special privileges are needed for auditing, software development, software installation, or other defined needs, they:
  - (1) Shall be authorized by the Information Owner or Custodian;
  - (2) Shall be created with an expiration date when supported;
  - (3) Shall be removed and disabled when work is complete.
- g. Investigations of users and their misuse of an information resource shall only be performed under the direction of the Information Security Office and/or the CIO.

### **4. Backup and Business Continuity**

**Authority-TAC: 202.75.7.D, 202.74**

The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by the Information Owner.

- a. The vendor(s) providing offsite backup storage for the university shall be approved to handle the highest level of information stored.
- b. Physical access controls implemented at offsite backup storage locations shall meet or exceed the physical access controls of the source systems. Additionally, backup media shall be protected in accordance with the highest university sensitivity level of information stored.
- c. A process shall be implemented to verify the success of the university electronic information backup.
- d. Backups shall be periodically tested to ensure that they are recoverable.
- e. Procedures between the university and the offsite backup storage vendor(s) shall be reviewed at least annually.

## **5. Change Management**

**Authority-TAC 202.75.7.E**

Changes which include additions, modifications and deletions to hardware, software, system components, services, and environmental facilities shall comply with the following:

- a. Review by technical assignee's management prior to implementation.
- b. Review by Information Owner representative prior to implementation.
- c. Prior communication of any scheduled outages.
- d. Proper back out and recovery procedures are utilized.
- e. Changes are logged and include appropriate information.
- f. Weekly reviews are conducted to evaluate and coordinate proposed changes.

## **6. Security Incident Management**

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

- a. Incidents involving computer security shall be managed by the Information Security Office and shall be reported as required by federal or state law or regulation (including Texas Department of Information Resources' requirements for security incident reporting).
- b. All unauthorized or inappropriate disclosures of Category-I data shall be reported promptly to the Information Security Office (security@angelo.edu or 325-942-2333).
- c. The university shall disclose, in accordance with applicable federal or state law, incidents involving computer security that compromise the security, confidentiality, and/or integrity of personal identifying information it maintains to Information Owners and any resident of Texas whose personal identifying information was, or is reasonably believed to have been, acquired without authorization.

Disclosure shall be made as quickly as possible upon the discovery or receipt of notification of the incident 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 that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency notifies the Information Security Office of their determination that it will not compromise the law enforcement investigation.

## **7. Network Access**

**Authority-TAC: 202.75.7.J, 202.77.a**

To maintain a high level of security and performance for the services on the university network, all users have the responsibility to:

- a. Acknowledge and abide by all policies set forth in the acceptable use policy.
- b. Provide proper account credentials or utilize publicly accessible services in accordance with their deployed purpose.
- c. Utilize only network addresses provided by infrastructure services.
- d. Utilize only those remote access services provided by infrastructure services.
- e. Not maintain connections to external networks while connected to the university network.
- f. Not extend or retransmit network services in any way.
- g. Not alter network hardware or software in any way.
- h. Not configure wireless personal area networks.
- i. Adapt all non-university owned systems to conform to networking standards.

## **8. Network Configuration**

**Authority- TAC: 202.75.7.K, 202.75.7.W**

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

- a. Design, deployment, and support of all network infrastructure and wiring for the university.
- b. The installation of all communications cabling.
- c. Approving configuration changes to network infrastructure.
- d. Alterations to network hardware and cabling.
- e. Extensions of network hardware and software.

- f. Establishment and management of all protocols used on the university network.
- g. Network address allocation and distribution.
- h. All connections to third party data and telephony networks.
- i. Installation and configuration of all network firewalls.
- j. Configuration and broadcast of all wireless signals providing access to the university network.
- k. Creation and maintenance of all university network infrastructure standards and guidelines.

## **9. Passwords**

**Authority- TAC 202.75.7.L**

### **a. Password Quality**

- (1) All account passwords shall comply with the following minimum password complexity requirements:
  - (a) Account passwords shall be at least 7 characters in length;
  - (b) Account passwords shall be changed every 120 days
- (2) Account passwords associated with Category-I data shall also comply with the following minimum password complexity requirements:
  - (a) Be at least 8 characters in length; and
  - (b) Contain a mixture of uppercase and lowercase letters, numerals, and special characters; and
  - (c) NOT re-use any of the account's last 24 passwords; and
  - (d) NOT include personal information such as your name and account name

### **b. End User Accounts**

- (1) Where possible, systems shall 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 shall be vetted when issuing an account or resetting a password.
- (3) Password changes shall comply with password strength requirements associated with the data classification of the service in question, where supported by the underlying accounting mechanism.

c. Identity Credentials

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

**10. Physical Access**

**Authority-TAC: 202.75.7.M; 202.73**

- a. All physical security systems shall comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- b. All information resource facilities shall 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 shall include the approval of the person responsible for the facility.
- d. Access cards and/or keys shall 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 shall be returned to the appropriate university department.
- f. Lost or stolen access cards and/or keys shall be reported immediately.
- 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 are kept for review.
- i. The card and/or key access rights of individuals that change roles or are separated from their relationship with the university shall be removed.
- j. Where applicable, alarm codes shall be assigned to staff and approved vendors as determined necessary by the person responsible for the facility.
- k. Alarm codes are not to 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 shall be reviewed at least annually.
- n. The State Office of Risk Management will be referred to for applicable rules and guidelines.

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

- o. Access to information resource facilities shall be granted only to university support personnel, and contractors, whose job responsibilities require access to that facility.

- p. Visitor access to information resource facilities shall be tracked with a sign in/out log.
- q. Visitors to card access controlled information resource facilities shall be escorted.
- r. Each individual that is granted access rights to an information resource facility shall sign the appropriate access and non-disclosure agreements.
- s. Information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.

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

- t. Category-I information shall not be stored on computing hardware in information resource facilities defined as computer labs.
- u. User validation is required before granting access to computing equipment in information resource facilities defined as computer labs.

## **11. Portable Computing**

**Authority-TAC 202.75.7.N**

- a. Portable computing devices used to access university information resources should be password protected.
- b. Sensitive data shall not be stored on portable computing devices. Specific permission shall be obtained from the Information Owner before a user may store category-I university data on a portable computing device.
- c. Sensitive data shall not be transmitted to/from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are used.

## **12. Privacy of Electronic Information**

**Authority-TAC 202.75.7.O**

- 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 shall follow the university standard formal request process. (Refer to OP 01.02.)
- b. The university may log, review, capture, and otherwise utilize 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, 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 shall be removed before sharing collected information to prevent loss of individual privacy where possible.
- d. Employees, contractors, vendors, and affiliates of the university shall safeguard the privacy and security of any information owned by or entrusted to the university.

### **13. Security Monitoring**

**Authority-TAC 202.75.7.P**

- 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 shall be consistent with system risk. All controls used should be tested.
- 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 all administrator and root access should be consistent with security risk.
- f. Any security issues discovered during log review or alerting shall be reported to the Information Security Office for follow-up investigation.

### **14. Security Awareness and Training**

**Authority-TAC: 202.75.7.Q; 202.77.a; 202.77.d-e**

- a. All users, including students and employees, shall 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 shall be provided at least annually to employees and students.
- c. The Information Security Office shall develop required technical training for employees providing support of information resources.

### **15. System Hardening**

**Authority-TAC 202.75.7.R**

- a. A server shall not be connected to the university network until it is in a university IT secured state and the network connection is approved by the Information Technology department.
- b. The degree of hardening for applications shall be in accordance with the importance of the information and the acceptable risk as determined by the Information Owner.
- c. Security controls shall be changed from manufacturer's factory settings before being places into operation.

- d. Security issues shall be monitored both internal and external to the university.
- e. Security patches shall be tested against IT core resources before release where practical.
- f. Where practical, hardware resources shall be made available for testing security patches.
- g. Security patches shall be implemented within the specified timeframe of notification from the Information Technology department.
- h. Appropriate login banners shall be placed at connection points to systems to identify that access is allowed only per this document.
- i. Systems designated for public access shall be configured to enforce security policies and procedures without the requirement for formal acknowledgement.

## **16. Software Licensing and Copyright**

**Authority-TAC 202.75.7.S**

- a. Copies of software licensed by the university shall not be made without verifying that a copy is permitted via the license agreement.
- b. Software used on university-owned systems shall be properly licensed for their method of use (concurrent licensing, site licensing, or per system licensing).
- c. The university has the right to remove inappropriately licensed software from university computers if the user is not able to show proof of license.

## **17. System Development and Acquisition**

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

- a. Mission critical software implementations shall use the Information Technology Project Office standard to address a preliminary analysis, risk identification, university goal alignment, planned timeframe, scope, and budget.
- b. All production systems shall have designated Information Owners and Custodians.
- c. Where resources permit, separation between the production, development, and test environments shall exist. Development and test environments containing production data shall require the same security protections as production systems.
- d. Patches and upgrades of system, database, or application software shall be installed and fully tested in a test environment, when available, prior to being installed in a production environment.
- e. Critical patches shall be applied on a regular basis and non-critical patches shall be applied as needed.
- f. Changes or upgrades to a production system shall follow a standard methodology.

## **18. Vendor Access**

### **Authority-TAC 202.75.7.U**

- a. Vendors shall comply with all applicable university policies and agreements.
- b. Vendor agreements and contracts shall specify:
  - (1) The university information resources to which the vendor should have access.
  - (2) How the university information is to be protected by the vendor.
  - (3) Acceptable methods for the return, destruction, or disposal of the university information in the vendor's possession at the end of the contract.
  - (4) The vendor shall only use university data and information resources for the purpose 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 to others.
- c. Each the vendor with access to university category I data shall be approved to handle that information.
- d. If vendor is involved in university security incident management, the responsibilities of the vendor shall be specified in the contract.
- e. Vendors shall observe regular work hours and duties as requested. Work outside of defined parameters shall be approved by appropriate university personnel.

## **19. Affiliated Organizations**

### **Authority-University Policy (OP 14.13)**

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

## **20. Malicious Code**

### **Authority-TAC 202.75.7.V**

- a. All workstations and servers, whether connected to the university network or standalone, shall use Information Technology approved anti-malware software and configuration.
- b. The anti-malware software shall not be permanently disabled or bypassed.
- c. The settings for the anti-malware software shall not be altered in a manner that will reduce the effectiveness of the software.
- d. The automatic update frequency of anti-malware software shall not be altered beyond the maximum update frequency standard maintained by the Information Technology department.

- e. Any system identified as a security risk due to a lack of anti-malware software may be disconnected from the network, or the respective network account may be disabled, until adequate protection is in place.
- f. Viruses not automatically cleaned by the anti-malware software constitute a security incident and shall be reported to the Help Desk.

## **21. Vulnerability Assessment**

**Authority-TAC 202.75.7.X**

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

## **22. Data Classification and Risk Assessment**

**Authority-TAC: 202.75.2, 202.72**

- a. Information Owners or designated Custodians, shall be responsible for classifying Digital Data processed by systems under their purview based on data sensitivity so that the appropriate security controls can be applied.
- b. The Data Classification Standard shall be used to identify digital data that is sensitive.
- c. A data classification of Category-I shall be based on compliance with applicable federal or state law, a contract, or on the demonstrated need to:
  - (1) Document the integrity of that digital data (that is, confirm that data was not altered intentionally or accidentally),
  - (2) Restrict and document individuals with access to that digital data, and
  - (3) Ensure appropriate backup and retention of that digital data.
- d. Certain digital data not defined as Category-I digital data can be so classified if warranted by a school or department's demonstrated need. With suitable justification, the university may convert its classification of these digital data from Category-I digital data to a lesser classification upon request by the Information Owner, with appropriate review and approval.
- e. Under the guidance of the Information Security Office, the university shall conduct and document an information security risk assessment annually according to state regulatory guidelines. ASU will rank inherent risk as High, Medium, or Low and perform biennial assessments for Medium and Low risks and annually for High risks.
- f. The confidentiality, integrity, and availability of information resources shall be managed and protected based on sensitivity and risk.

## **23. Protection and Privacy of Personally Identifiable Information**

**Authority-TAC 202.78**

- a. Disclosure of personally identifiable information to unauthorized persons or entities is expressly forbidden.
- b. Efforts shall be made to reduce the collection and use of personally identifiable information. If the information is required to be collected by state or federal law, the individuals shall be informed of the requirement on the form or at the time of collection.
- c. Access to personally identifiable information shall be granted through an appropriate approval process and be revalidated on a regular basis.
- d. Paper and electronic documents containing personally identifiable information shall be secured during use and when not in use.
- e. Electronic documents containing personally identifiable information shall only be stored on authorized systems.
- f. Any paper or electronic document containing personally identifiable information (or media containing such documents) shall be disposed of in a secure manner. Disposition of electronic media shall meet TAC 202.78 requirements.
- g. Safeguards shall be adopted to protect personally identifiable information in business office environments and on systems/devices that contain such information.

#### **24. Disciplinary Action**

Violation of this policy may result in disciplinary action which may lead up to or include termination for employees and temporaries; a 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 Angelo State University information resources access privileges, and civil or criminal prosecution.