TEXAS A&M UNIVERSITY
SAN ANTONIO

29.01.03.00.01.S2 Information Security Responsibilities of Owners and Custodians

Approved: August, 2019
Next Scheduled Review: August, 2024

Table of Contents

STANDARD STATEMENT

The Information Security Officer (ISO) issues this Standard pursuant to Texas A&M University-San Antonio (A&M-San Antonio) Procedure 29.01.03.00.01 *Information Security* to specify the information security responsibilities of Owners and Custodians. The responsibilities this Standard imposes supplement the User responsibilities in Standard 29.01.03.00.01.01 *Information Security Responsibilities of Users*.

REASON FOR STANDARD

This Standard applies to Owners and Custodians of electronic information resources belonging to A&M-San Antonio.

This Standard provides measures to mitigate information security risks associated with Administrator Access. Information Resource Owners or department or division heads may provide additional measures to mitigate risks. The ISO shall assess potential risks

and appropriate mitigation measures in collaboration with the Information Resource Manager (IRM), Information Resource Owners, and/or department or division heads. In accordance with Texas Administrative Code 202 - Information Security Standards (TAC 202), a department, division, or resource owner may elect not to implement a risk mitigation measure in this Standard based on a documented analysis of the risks and business functions at issue. A department, division, or resource owner must give notice to the ISO of a decision to forego full or partial implementation of a risk mitigation measure. A decision to forego implementation is not effective until the ISO receives, accepts, and acknowledges the risk management decision in writing. All risk management decisions must be documented in the annual security assessment report.

Official Standard

Account Management

1. Standard Statement

    1.1. A&M-San Antonio information resources are strategic assets, which being property of the State of Texas, must be managed as valuable state resources. Computer accounts provide a means of providing access, a key to any computer security program, and for Information Resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

    1.2. This Standard applies to all A&M-San Antonio Information Resources.

2. Official Responsibilities

    2.1. An approval process is required prior to granting access authorization to an Information Resource. The approval process shall document the acknowledgement of the account holder to follow all terms of use and the granting of authorization by the resource owner or their designee.

2.2. Each person is to have a unique Logon ID and associated account for accountability purposes. Role accounts (e.g., guest or visitor) are to be used in very limited situations and must provide individual accountability, which also includes wireless access to Information Resources.

2.3. Access authorization controls are to be modified appropriately as an account holder's employment status or job responsibilities change.

2.3.1. Account creation processes are required to ensure that only authorized individuals receive access to Information Resources.

2.3.2. Processes are required to disable Logon IDs that are associated with individuals that are no longer employed by, or associated with A&M-San Antonio. In the event that the access privilege is to remain active, the department (e.g., owner, department head) shall document that a need or benefit to the university exists.

2.3.3. All access privileges to Information Resources must be reviewed at least annually by the owners (department heads or administrators), and documented as such.

2.3.4. All Logon IDs having access to mission critical and/or confidential resources that have not been used/accessed within a period of six (6) months, may be disabled at the discretion of the Information Resource Owner, Information Technology Services (ITS), or the University's ISO. Exceptions can be made where there is an established departmental procedure.

2.4. Passwords associated with Logon IDs shall comply with the university system password management procedure.

ADMINISTRATOR ACCESS

1. Standard Statement

   Technical support staff, security administrators, system administrators, and others may have special access account privilege requirements compared to typical users. Administrator accounts and other special access accounts have extended and overarching privileges in comparison with typical users. Thus, the granting, controlling, and monitoring of these accounts is extremely important to an overall security program. The purpose of the university administrator access management procedure is to establish the process for the creation, use, monitoring, control, and removal of accounts with special access privilege.

2. Official Standard

   2.1. All Department Heads and Information Resource Owners shall maintain a list(s) of personnel who have administrator access accounts for hosted or local departmental information resources systems. The list(s) shall be reviewed with the ISO at least annually by the appropriate division/department head, director, or their designee.

   2.2. In the course of normal duties, employees with administrator access privileges may access descriptive data to review various events related to the performance or security of those resources. Authorized ITS personnel may also routinely review events related to the performance and secure operation of the A&M-San Antonio network. System Administrators may at times also access user data in maintaining the operational integrity and security of information resources. System Administrators shall, however, maintain the confidentiality of user data to the extent possible and not divulge user data except to authorized University officials (such as described in 3.1).

   2.3. Use of administrator access privileges to conduct personnel related investigations shall be directed by appropriate University and Texas A&M University System (System) management personnel (e.g. Dean, Vice President, President, System Internal Audit, Office of General Counsel).

2.4. Activities conducted beyond the normal duties outlined in Item 2 above (Responsibilities) involving user data shall insure that any user data is revealed only to third parties as outlined in Item 3 (Responsibilities). Compliance with all privacy laws is required (e.g. Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, and the Texas Public Information Act).

2.5. In those cases where law enforcement agencies request access in conjunction with an investigation, the request shall be in writing (e.g. subpoena, court order). All such requests shall be reported to the appropriate division/department head, or their designee upon receipt and the system Office of General Counsel.

2.6. Each individual that uses administrator access accounts shall use the account or access privilege most appropriate for the requirements of the work being performed. Privileged accounts may not be used for normal user activities, only for the privileged functions designated by the account.

2.7. All users who need local administrator access to workstations must complete the process for establishing administrative privileges (see form "Administrative Privileges for Workstation MOU").

2.8. Each account used for administrative access must follow requirements established in SAP 29.01.03.00.25 "Password Authentication".

2.9. Each individual that uses administrator access accounts will refrain from abuse of privilege and shall only conduct reviews as directed by appropriate university management personnel or IRM.

2.10. The password for a shared administrator access account shall change under the following conditions:

2.10.1. An individual knowing the password leaves the university or department;

2.10.2. Job duties change such that the individual no longer performs functions requiring administrator access;

2.10.3. A contractor or vendor with such access leaves or completes their work;

2.10.4. Shared administrator passwords will be changed a minimum of every six (6) months if a previously listed event does not trigger a prior password change

2.11. In the case where a system has only one administrator, there must be a password stored in a secure space (safe or vault) in an envelope such that an appropriate individual other than the administrator can gain access to the administrator account in an emergency situation.

2.12. When special access accounts are developed for internal or external audits, software development, software installation, or other defined needs, they must be:

2.12.1. Authorized by a department head;

2.12.2. Created with a specific expiration date; and,

2.12.3. Removed when the task or project is complete.

3. Forms

Administrative Privileges for Workstation MOU

Application Security

1. Standard Statement

Application development security measures must be taken throughout an application's life cycle in order to build more secure and robust applications. When a web application's design begins, it is essential to apply threat risk modeling;

otherwise, resources, time and money will be consumed on useless controls that fail to focus on the real risks.

2. Reason for Standard

    2.1. This Standard applies to all users of A&M-San Antonio information resources.

    2.2. The purpose of the implementation of this Standard is to serve as a framework for developing, deploying and maintaining secure applications.

    2.3. This Standard is intended for all developers, security testers and system architects developing and/or administering applications to process A&M-San Antonio data.

3. Official Responsibilities and Standard

    3.1. ITS should be notified or involved in any work related to the development or deployment of applications at A&M-San Antonio.

    3.2. The ISO must always have a full inventory of all web applications.

    3.3. ITS must ensure that a security risk assessment of the system is performed prior to moving the application to production. The application owner is responsible for resolving all security related risks and vulnerabilities prior to ITS certifying the application as ready for production.

    3.4. Security scans must be performed at least annually after deployment in order to identify vulnerabilities.

Backup and Recovery

1. Standard Statement

    Electronic backups are required to enable data and application recovery and availability in case of natural disasters, system disk drive failures, corruption, data

entry errors, system operations errors, or other unforeseen events. This Standard establishes the process for the backup and storage of information resources.

2. Reason for Standard

   This Standard applies to all A&M-San Antonio resources that contain mission critical information.

3. Official Standards

   3.1. The extent of backups shall be determined by the importance of the information, potential impact of data loss/corruption, and risk management decisions by the data owner. Backups shall be stored on backup media, redundant disk drives, and/or virtual tape libraries. Activities from the annual risk assessment will assist in identifying this importance.

   3.2. Mission critical information backup and recovery processes for each system, including those for offsite storage, must be documented and reviewed periodically.

   3.3. Physical access controls implemented for on or offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additional backup media must be protected in accordance with the highest sensitivity level of the information stored.

   3.4. Backups shall be periodically tested to ensure that they are recoverable.

   3.5. Physical and logical authentication mechanisms used for permitting access to University backup applications and media must be reviewed annually or when an authorized individual leaves the University.

   3.6. Any vendor(s) providing offsite backup or backup storage for University information resources must be cleared to handle the highest level of information stored. Standards between the university and the offsite backup or backup storage vendor(s) must be reviewed at least annually.

3.7. Backups of system that contain, or may contain, sensitive information must be encrypted and stored in a secure, environmentally safe, locked facility accessible only to authorized University approved representatives (TAC 202.74(b) and the keys associated with the encryption mechanism must be escrowed in a secure location.

3.8. All backup media shall be preserved for the appropriate retention period prior to being overwritten for reuse.

Change Management

1. Standard Statement

1.1. As Information Resources expand and become more complex, A&M-San Antonio must have a strong change management process.

1.2. Information resources may require planned upgrades or maintenance that call for system downtime or outages. Unplanned outages may occur that necessitate upgrades or maintenance to information resources. Change stemming from planned or unplanned upgrade, maintenance, and outages is a critical part of providing technology support services for the University.

2. Reason for Standard

2.1. The purpose of the implementation of this Standard is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community.

2.2. This Standard applies to all individuals who install, operate or maintain A&M-San Antonio information resources.

3. Official Responsibilities and Standard

3.1. Change Management Protocols:

3.1.1. The following change management protocols apply to the department of ITS, as well as all campus departments. A change has a possibility of impacting normal operations on information resources. Items that are considered changes include, but are not limited to:

3.1.1.1. Installation or upgrades of server, networking, or security hardware or software, including patches and updates for the applications.

3.1.1.2. Modification of hardware or software that affects the operation of desktop computers connected to A&M-San Antonio's network.

3.1.1.3. Modification of server, network, or security settings that affect access to ITS IR.

3.1.1.4. Modification or enhancements to the physical environment that supports ITS IR.

3.1.2. Specific tasks that should not be considered changes include:

3.1.2.1. Updates to operating systems,

3.1.2.2. Creation of new file shares or modification to permissions of existing shares,

3.1.2.3. Installation, activation, or removal of network cable drops, or

3.1.2.4. Creation, modification, or deletion of accounts and mailboxes.

3.2. Change Management Process:

3.2.1. All changes must be documented and submitted for approval prior to implementation. The following defines the Standard for documentation and approval:

3.2.1.1. The custodian requesting the change must fill out a Change Management Request email to obtain approvals.

3.2.1.2. Requestor will submit the email to the CIO and Directors for review. The CIO and Directors will work with necessary stakeholders ensure accuracy, completeness, and identify potential impacts. Change forms must be submitted a minimum of one full business day prior to the review date.

3.2.1.3. If appropriate, announcement messages should be distributed to users prior to the changes.

3.2.1.4. Changes to critical systems must be done in a test environment first, if available.

3.2.1.5. Once a change has been done, the Application Custodian needs to test the system in order to ensure the integrity of the system.

3.2.1.6. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability requiring immediate attention.

Incident Management

1. Standard Statement

This Standard describes the requirements for dealing with computer security incidents. Security incidents include, but are not restricted to: malicious code

detection; unauthorized use of computer accounts and computer systems; theft of computer equipment or theft of information; accidental or malicious disruption or denial of service as outlined in security monitoring Standards, intrusion detection Standards, internet/intranet Standards, and acceptable use Standards. Incidents, deemed to be severe or repetitive, should be reported to either the Chief Information Officer (CIO) or the ISO as soon as possible. Once an incident is reported the CIO and ISO will determine the severity of the incident, and categorize it appropriately.

2. Reason for Standard

   This Standard provides a set of measures that will mitigate information security risks associated with incident management and describes the requirements for dealing with computer security incidents. It applies to all individuals who use Texas A&M University -San Antonio (A&M-San Antonio) information resources.

3. Official Responsibilities and Standard

   3.1. Incident Management Standards:

   3.1.1. The ISO is responsible for initiating, completing and documenting any and all incident investigations.

   3.1.2. Upon discovery of an incident the ISO is responsible for notification to, but not limited to, the IRM, DIR, University administration, or other law enforcement, as applicable. At a minimum, the ISO will provide the IRM with regular reporting of all incidents discovered and/or reported to ITS. In addition, all incidents are required to be submitted monthly to the DIR.

   3.1.3. Faculty/Staff/Students that identify a security incident should immediately contact the ITS Help Desk and/or ISO.

   3.1.4. In cases where law enforcement is not involved, the ISO will recommend corrective or disciplinary actions, if appropriate, to the IRM. The IRM will review and submit through the appropriate vice president or executive team member.

3.1.5. Any incident that involves criminal activity under Texas Penal Code Chapters 33 (Computer Crimes) or 33A (Telecommunications Crimes) must also be reported to the University Police Department (UPD).

3.1.6. For incidents directly involving A&M-San Antonio employees, the Human Resources department and the appropriate vice president or dean will be contacted.

3.1.7. For incidents directly involving A&M-San Antonio students, the Division of Student Affairs will be contacted.

3.1.8. The ISO is responsible for determining and coordinating the gathering the physical and electronic evidence necessary for the incident investigation.

3.1.9. The ISO and IRM will determine if a campus wide notification is required, the content of the communication and how best to distribute the communication.

3.1.10. The ITS security team is responsible for ensuring that any damage from a security incident is repaired.

3.2. Incident Categorization:

CATEGORY	DESCRIPTION	EXAMPLES
Level 1	Least severe and most common type of incident. Typically lacks a widespread effect on University functions.	• Minor policy violations by an employee. • Detection and removal of viruses or malware.
Level 2	No impact on overall business functions and small impact on operational functions.	• Repeated reconnaissance activity from the same source. • Attack blocked by the University's security

CATEGORY	DESCRIPTION	EXAMPLES
		Infrastructure. • Regular occurrence of Level 1 incidents. • Successive attempts to gain unauthorized access to a system.
Level 3	Impact on the University's ability to meet its mission objectives, major impact on business or operational functions. Risk of damage to University reputation or financial loss.	• Unauthorized access to sensitive systems. • Improper use of high level accounts such as root or administrator. • Defacement of A&M-San Antonio web site. • Denial of service attacks • Unauthorized changes to key infrastructure. • Theft/Loss of computer systems, or media, containing sensitive information or confidential information. • IT related PCI, HIPAA or FERPA violations.

PHYSICAL ACCESS

1. Standard Statement

   Technical support staff, security administrators, system administrators and others, may have physical facility access to information resource as part of their job responsibilities. The granting, controlling and monitoring of the physical access to information resources facilities is extremely important for overall security and protection of University assets

2. Official Responsibilities and Standard

2.1. All facilities supporting information resources must be physically protected in proportion to the criticality and confidentiality of their function and the information contained with the physical location.

2.2. The process for granting card and physical key access to information resources facilities must include the approval of the IRM.

2.3. The department that issues the access card or physical key (i.e. facilities, ID Card Office, UPD, or CIO) will be responsible for maintaining proper documentation. Access to facilities or locations that contain information resources must be approved by the IRM.

2.4. Access to Information Resources facilities must be granted only to A&M-San Antonio support personnel and contractors, whose job responsibilities require access to that facility.

2.5. Access cards and physical keys must not be shared with others.

2.6. Visitors must be escorted by staff personnel with clearance in card access controlled areas of information resources facilities.

2.7. All physical security systems must comply with applicable regulations, including but not limited to, building codes and fire prevention codes.

2.8. Signage for restricted access rooms and locations must be practical. Minimal discernible evidence of the importance of the location should be displayed.

2.9. Access cards and physical keys that are no longer required must be immediately returned to the issuing office by the employee (i.e. facilities, ID Card Office, UPD, or CIO). Cards must not be reallocated to another individual bypassing the return process. As part of the termination process, it is the supervisor's responsibility to ensure that all access cards and physical keys are returned.

2.10. Lost or stolen access cards and physical keys must be immediately reported to the issuing department (i.e. facilities, ID Card Office, UPD, or CIO) and ISO or IRM.

2.11. Physical access records shall be maintained as appropriate for the criticality of the Information Resources being protected. Such records shall be reviewed as needed by the Information Resources Manager (IRM).

Firewall Management

1. Standard Statement

   Firewalls prevent unauthorized access to or from a private network and are a fundamental element of the University's information systems security infrastructure. Firewalls regulate and control network connectivity and necessary Internet services such as web browsing, mail services, and file transfers. Firewalls establish a perimeter where access controls are enforced.

2. Official Responsibilities and Standard

   2.1. All A&M-San Antonio Internet access will be consolidated and provided through a perimeter firewall and a centralized information technology infrastructure. Individual divisions, departments, and/or colleges should not establish independent Internet connectivity outside of the centralized information technology infrastructure. All requests for independent Internet connectivity will be directed to ITS and must be approved by the Information Resources Manager (IRM).

   2.2. The ISO will be responsible for providing guidance and direction for A&M-San Antonio firewall architecture, inbound/outbound protocols, traffic monitoring, and approval of any updates or changes to firewall rules. Enforcement of firewall and DMZ rules is the responsible of the ISO.

   2.3. ITS is responsible for monitoring and configuration of all firewall rule sets. The A&M-San Antonio ISO is responsible for enforcing all applicable firewall policies. The ISO shall coordinate with the State of Texas Department of

Information Resources (DIR) or approved vendor to conduct annual controlled penetration testing and web server application vulnerability assessments. Formal reports generated from these tests will be delivered to the IRM. All corrections and enforcement of changes will be coordinated by the ISO.

2.4. All A&M-San Antonio perimeter firewalls shall be hardware appliances that provide a separate layer of architecture between the internal and external network. Perimeter firewalls shall be redundant and configured in an active/failover topology.

2.5. All A&M-San Antonio firewalls must be located in a secure location with controlled and monitored access.

2.6. The A&M-San Antonio perimeter firewall permits all outbound (egress) and inbound (ingress) traffic to Internet services with the exception of network traffic that violates A&M-San Antonio policy, state, and/or federal laws. Network traffic that contains unauthorized services, viruses, worms, or other malware may be blocked at any time to protect the integrity and reputation of A&M-San Antonio.

2.7. Alarm and alert functions as well as audit logging of any and all firewalls and/or other network perimeter access control systems shall be enabled.

2.8. All firewall activity shall be monitored and logged to ensure compliance with University policy, state, and/or federal laws. Additional logging devices and/or other third party inspection appliances may be used to provide further analysis and monitoring.

Security Awareness and Training

1. Standard Statement

Understanding the importance of information security, individual responsibilities, and accountability pertaining to information security are paramount to achieving organization security goals. This can be accomplished with a combination of general information security awareness training and targeted, product-specific training. The

security awareness and training information is a continuous effort and will be updated as needed. The purpose of the security training Standard is to describe the requirements to ensure each user of university information resources receives adequate training on information security issues.

2. Official Responsibilities and Standard

2.1. All University personnel who use information resources are required to comply with the Standards outlined in this Standard. All Department Heads and Information Resource Owners shall ensure completion of security awareness training on an annual basis, provided through SSO. Additional training may be required by the IRO and assigned to identified personnel as they see fit.

2.1.1. All new employees shall complete security awareness training prior to, or at least within 30 days of, being granted access to any University information resources. This shall be part of the new employee's orientation training session.

2.1.2. All users shall acknowledge completion of university security awareness training on an annual basis.

2.2. Information technology personnel shall establish security program in addition to making relevant security information available to owners and users of information resources.

2.3. The Information Resource Owners may oversee the preparation, maintenance, and distribution of information security manuals or supplemental information security training that describe how university rules and Standards relate to the security of departmentally owned information resources. All manuals and/or supplemental documents are to be provided to the University ISO for reference and proper records retention.

INTERNET/INTRANET USE

1. Standard Statement

   1.1. A&M-San Antonio supports and encourages internet and intranet use for all users of information resources. Information resources are strategic assets of the State of Texas and must be managed as valuable state resources. A&M-San Antonio establishes this Standard to achieve the following:

      1.1.1. Ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;

      1.1.2. Establish acceptable practices for the use of information resources; and

      1.1.3. Educate individuals who may use information resources with respect to their responsibilities.

2. Official Responsibilities and Standard

   2.1. All Internet and Intranet usage by University employees, authorized vendors, business partners, students, and guests must adhere to federal and state laws, as well as System and University policies, regulation, rules, procedures, and Standards.

   2.2. Users are responsible for their account(s). Users should make appropriate use of the system(s) and network-provided features to ensure computer resources are protected.

   2.3. Users must not use another user's account or password without proper authorization. Individual password security is the responsibility of each individual user.

   2.4. Users are prohibited from using any form of electronic media (e.g. email or web resource) to harass, intimidate, or otherwise annoy another person/group.

2.5. University Internet or Intranet access may not be used for personal gain or solicitations.

2.6. All activity may be subject to logging and review.

2.7. No University mission critical or confidential information shall be made available via University websites or public websites without ensuring that the material is accessible to only authorized individuals or groups.

2.8. ITS and/or other department heads in control of information resources are required to ensure that all systems and software accessing the Internet and Intranet are up-to-date with security patches and the system's protection software are maintained.

2.9. Downloading games, music, movies or any other non-business software or materials may be restricted by ITS for network performance purposes.

2.10. All sensitive material transmitted over external networks must be encrypted.

2.11. Any security violations, and unauthorized use pertaining to this Standard, shall be reported according to the ISO and/or the IRM.

2.12. Incidental use of Internet/Intranet access is subject to A&M-San Antonio Standard, 29.01.03.00.02. Acceptable Use for Information Technology. Incidental use definitions apply to all Internet/Intranet activities to include downloading.

Encryption of Confidential and Sensitive Information

1. Standard Statement

1.1. TAC §202.71(b) requires institutions of higher education to define data classification categories and to establish appropriate controls for each category. Controls typically include user authentication, encryption, periodic scanning, and the sanitization of decommissioned or repurposed storage media. This Standard

defines the classification of A&M-San Antonio data and the controls to be implemented to protect such data.

2. Reason for Standard

2.1. This Standard applies to all A&M-San Antonio employees and affiliates, including contractors having confidential or sensitive data in their possession or under their direct control (e.g. manages the storage device) to ensure that appropriate risk mitigation measures (e.g. encryption) are in place to protect data from unauthorized exposure.

2.2. It addresses encryption requirements and controls for confidential and/or university-sensitive data that is at rest (including portable devices and removable media) regardless of ownership of the particular storage device, and data in motion (transmission security). This Standard is compatible with, but does not supersede or guarantee compliance with all State and federal encryption standards.

2.3. When encryption is used, appropriate key management Standards are crucial. Anyone employing encryption is responsible for ensuring that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.

3. Official Standard

3.1. All encryption mechanisms implemented to comply with this Standard must support a minimum of, but not limited to, FIPS-Compliant 128-bit encryption. The use of proprietary encryption algorithms is not permitted for any purpose unless reviewed and approved by the Information Resources Manager (IRM) and/or A&M-San Antonio ISO.

3.2. Recovery of encryption keys will be part of business continuity planning where applicable and appropriate except for data used by a single individual.

3.3. When A&M-San Antonio storage media is de-commissioned or repurposed, computer hard drives or other storage media that have been encrypted shall ensure that the media is either 1) physically destroyed by shredding or other accepted practice 2) be sanitized in accordance with TAC §202.78, removal of data from data processing and storage equipment to prevent unauthorized exposure.

3.4. Sensitive or confidential A&M-San Antonio data must not be stored on portable computing devices. However, in the event that there is no alternative, such data must be encrypted using university-approved encryption techniques and reviewed and approved by the IRM and/or ISO. Contact the ITS Helpdesk for assistance with encryption.

3.5. Sensitive or confidential A&M-San Antonio information must not be transmitted via wireless, including Bluetooth, to or from a portable computing device unless encryption techniques are utilized.

3.6. Remote access to A&M-San Antonio systems must utilize approved encryption techniques when transmitting or receiving sensitive or confidential information.

3.7. Any confidential or sensitive A&M-San Antonio data transmitted to or from a site not on the campus network (e.g. to and from vendors, customers, or entities doing business with A&MSan Antonio) must be encrypted and transmitted through an encrypted tunnel or secure socket layer (SSL) connection.

3.8. Confidential or sensitive data transmitted via an email message must be encrypted.

3.9. Transmitting unencrypted confidential or sensitive data through the use of email programs is prohibited.

3.10. Transfer of confidential or sensitive documents and data over the Internet using approved secure file transfer protocols (e.g., HTTPS, “secured FTP”). This

transfer is permitted to users that are authorized to view the confidential or sensitive data only.

3.11. Before confidential or sensitive A&M-San Antonio data is transferred to an authorized third party (e.g. vendors or business partners), the third party must affirm that they will protect the transferred data in accordance with the conditions imposed by the data's owner. At a minimum, the conditions specified in this Standard will be adopted and used as the baseline for transfer activity.

Intrusion Detection

1. Standard Statement

1.1. A&M-San Antonio network infrastructure is provided as a central utility for all users of University information resources. Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information resources grow in complexity, effective security systems must evolve. Intrusion detection systems can provide part of this assurance.

2. Official Responsibilities and Standard

2.1. The University operates systems that are used to monitor, detect and log intrusion attempts via the IP network. These systems include intrusion detection systems, firewalls, email virus scanning, antivirus protection for servers and workstations. Anomalies will be investigated and appropriate measures will be taken in the event of an actual threat in accordance with 29.01.03.00.08 Incident Management.

2.2. All suspected and/or confirmed instances of host, server, or network intrusions will be reported immediately as outlined in 29.01.03.00.08 Incident Management to the ISO.

2.3. Operating system, user accounting and application software audit processes will be enabled on all host and server systems where resources permit.

2.4. Alarm and alert functions, as well as audit logging of any firewalls and other network perimeter access control systems will be enabled.

2.5. Logs from the firewalls and network perimeter access control systems will be monitored and reviewed as risk management decisions warrant.

2.6. Logs for servers and devices will be monitored and reviewed as risk management decisions warrant.

2.7. The ISO will work with the CIO/IRM to remediate any identified risk or intrusions to the A&M-San Antonio network.

Malicious Code

1. Standard Statement

   A&M-San Antonio information resources are strategic assets and must be managed as valuable state resources. Malicious code can disrupt normal operation of University information resources. This Standard is intended to provide information to administrators and users to improve the resistance to, detection of, and recovery from malicious code.

2. Official Responsibilities and Standard

   2.1. Prevention and Detection

      2.1.1. Information resources connected to the A&M-San Antonio network must be kept up-to-date with security updates from the manufacturer of operating system and application software (e.g. patched and updated).

      2.1.2. Dedicated firewall hardware and anti-virus software shall be utilized to protect information resources connected to the University network in the prevention of malicious code attacks/infections. Any information resource containing confidential information that cannot implement these safeguards should be reported to the A&M-San Antonio Information ISO and IRM.

2.1.3. Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed. Scanning should include files of unknown integrity on any electronic media (i.e. external hard drive, USB memory key, etc.).

2.1.4. The automatic update frequency of firewall and anti-virus software shall not be disabled, altered or bypassed to reduce the frequency of updates by any user.

2.1.5. Email servers and gateways must provide protection from malware, spam and phishing.

2.1.6. Whenever possible, the use of two-factor authentication should be considered and implemented.

2.1.7. Users are to notify ITS Help Desk in the event they feel that a virus may have infected their equipment.

2.2. Response and Recovery

2.2.1. ITS personnel should thoroughly document the incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information resources, and follow 29.01.03O0.08 Incident Management to report the incident.

2.2.2. All reasonable efforts shall be made to contain the effects of any system that is infected with a virus or other malicious code. This may include disconnecting systems from the network or disabling email accounts.

2.2.3. If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current anti-virus or other control software.

2.2.4. If malicious code cannot be automatically quarantined or removed by anti-virus software, the system shall be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact.

2.2.5. The presence of the malicious code shall be reported to the ITS Help Desk so that they may take appropriate actions in removing the malicious code and protecting other systems.

2.2.6. Personnel responding to the incident should have or be given the necessary access privileges and authority to affect the necessary measures to contain/remove the infection.

2.2.7. Utilize anti-virus, anti-spyware, etc. software to execute a complete system scan including the boot sector and all physical drives, to eradicate all malicious code that may be identified.

2.2.8. Any removable media (including diskettes, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.

Network Scanning and Vulnerability Assessment

1. Standard Statement

   Network scanning is frequently used to generate a network security report detailing possible vulnerabilities of the systems attached. The operating systems and applications for all information resource must undergo a regular vulnerability assessment in accordance with TAC 202 - Information Security Standard.

2. Reason for Standard

   The purpose of the implementation of this Standard is to gather information that will be used for network scanning and vulnerability assessment, including notifying owners of vulnerabilities, determining incorrectly configured systems, validating firewall access requests, and gathering network census data.

3. Official Responsibilities and Standard

    3.1. ITS will conduct network scans and network vulnerability scans of devices attached to the University network.

    3.2. Network scans or network vulnerability scans must be authorized by IRM or designee.

    3.3. Under no circumstances may network scanning be conducted by unauthorized users.

    3.4. Owners of information resources found to be vulnerable will be contacted by the ISO concerning the identified risk(s). The Information Resource Owner is responsible for ensuring that the identified risk(s) is mitigated in a timely manner.

    3.5. A vulnerability assessment will be conducted by DIR at least annually.

    3.6. Other exceptions to these guidelines may be authorized only by the A&M-San Antonio President, IRM, or designee.

Network Access

1. Standard Statement

    The network infrastructure is provided by A&M-San Antonio for all authorized users. It is important that network infrastructure, which includes media, active electronic equipment (i.e., routers, switches, cables, etc.) and supporting software, be able to meet current business performance requirements.

2. Official Responsibilities and Standard

    2.1. Management of network addresses, address space, and network naming will be managed by ITS. ITS is required to approve all access methods, installation of all network hardware, and requirements for attaching any computer system or device to the A&M-San Antonio operated network. This process ensures that

access to the network does not interfere with the operation and reliability of the network.

2.2. Users shall notify ITS when any network connected information resources have been transferred, replaced, or decommissioned.

2.3. Users are not permitted to extend or re-transmit network wired or wireless services in any way. Any network aggregation devices (e.g. hubs, switches, routers) shall be approved by the University ISO or the Information Resources Manager (IRM) before being connected to the network infrastructure.

2.4. Anonymous access to the network is not permitted.

2.5. Network management or other monitoring devices shall not be connected to network infrastructure without approval by the ITS department.

2.6. End-users shall not connect or install any information resource device that is not provided and supported by the University without approval by ITS. Additionally, end-users shall not alter or disable University network infrastructure devices or equipment.

2.7. Virus protection software must not be disabled or bypassed except as required by the temporary installation of software or for other authorized special circumstances.

2.8. Remote access to the University network is only authorized through approved and supported means (e.g. SSL VPN, VPN client, etc.) provided by ITS.

2.9. Remote access by contractors or vendors must be approved by the IRM and follow the Standard set forth in 29.01.03.00.26 Vendor Access.

2.10. Non-University computers or devices connecting to the network provided by the University must conform to all appropriate security standards for information resources.

2.11. ITS reserves the right to inspect any system or equipment connecting to the network and disconnect as necessary for business or other risk related reasons.

Network Configuration

1. Standard Statement

   The A&M-San Antonio network infrastructure is provided as a central utility for all users. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high-speed networking technology to allow the future provision of enhanced user services.

2. Reason for Standard

   This Standard applies to all A&M-San Antonio information resources. The purpose of this Standard is to establish the rules for the maintenance, expansion and use of the network infrastructure. This Standard is necessary to preserve the integrity, availability and confidentiality of A&M-San Antonio information resources. This Standard applies to all individuals with access to A&M-San Antonio information resources.

3. Official Responsibilities and Standard

   3.1. ITS is responsible for A&M-San Antonio networking infrastructure which includes all cabling, wireless signaling and connected electronic devices to ensure reliability of operations, proper accessibility to resources, and protection of data integrity.

   3.2. All hardware connected to an A&M-San Antonio supported or operated network is subject to ITS management and monitoring standards.

   3.3. ITS is responsible for ensuring the following are duties are performed in support of A&M-San Antonio network configuration:

      3.3.1. A&M-San Antonio network infrastructure configurations;

3.3.2. The management of any changes, adds, and enhancements to the University network;

3.3.3. Operating and maintaining a reliable network with appropriate redundancy requirement to meet quality of service goals;

3.3.4. Installing or authorizing a third-party vendor to install all cabling and network hardware;

3.3.5. Maintaining a list of network inventory connected to the A&M-San Antonio network;

3.3.6. Authorizing changes to the configuration of active network management devices;

3.3.7. Ensuring A&M-San Antonio firewalls are installed and configured following 29.01.03.O0.10 Firewall Management;

3.3.8. Users must not extend or re-transmit network services in any way. Network aggregation devices (i.e. router, switch, hub, wireless access point) must not be connected without ITS approval;

3.3.9. The use of departmental firewalls is not permitted without the written authorization from the A&M-San Antonio IRM.

Platform Management/Server Hardening

1. Standard Statement

   Servers are relied upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use,

and disruptions in service. Additionally, desktop computing systems must be secured and maintained to prevent similar unauthorized use and access.

2. Official Responsibilities and Standard

2.1. Standards for all Servers

2.1.1. Systems administrators will test security patches prior to implementation when practical. Systems administrators are encouraged to have hardware resources available for testing security patches in the case of special applications.

2.1.2. A server must not be connected to the A&M-San Antonio network until it is in an accredited secure state and the network connection is approved by network services personnel.

2.1.3. System Administrators shall ensure that vendor supplied patches are routinely acquired, systematically tested, and installed promptly based on risk management decisions.

2.1.4. System Administrators shall remove unused software, system services, and drivers as needed.

2.1.5. System Administrators shall enable security features included in vendor supplied systems including, but not limited to, firewalls, virus scanning and malicious code protections, and other file protections.

2.1.6. System Administrators shall enable audit logging, preferable to a central logging server, and shall review logs based on risk management decisions.

2.1.7. User privileges shall be set utilizing the least privileges concept of providing the minimum account of access required to perform job functions. Privileges may be added as need is demonstrated by the user and appropriate division/department head. The use of passwords shall be enabled in accordance with 29.01.03.00.25 Password Authentication

2.1.8. System Administrators shall disable or change the password of default accounts before placing the resource onto the network. The System Administrator will assign a "strong" password based on strong password standards on all default and/or administrative accounts.

2.1.9. Servers shall be tested for known vulnerabilities when new vulnerabilities are announced, and shall seek and implement industry security practices for securing their particular system platform(s). Upon notice of vulnerability, servers will be tested within 30 days.

2.2. Windows Servers

Microsoft Windows Server Update Services shall be utilized to provide automatic hotfixes, patches, service packs, and device drivers from a centralized IT server. In instances where automated update pools are unable to be utilized, manual updates will be performed as soon as reasonably possible based on risk management decisions.

Portable Computing

1. Standard Statement

Portable computing devices such as smart phones, tablets, laptop computers, USB memory (aka thumb drives) are becoming convenient, powerful and easy to use. Their small size and functionality are making these devices more desirable to replace traditional desktop devices in a wide number of applications. Portable computing devices also introduce risk to personal privacy and University data. This document outlines guidelines regarding the use of these portable computing devices in the A&M-San Antonio computing environment.

2. Official Responsibilities and Standard

2.1. Portable computing devices must be password-protected using the security feature provided on the tool, and there should be no sharing of portable computing device passwords.

2.2. Whenever possible, sensitive or confidential A&M-San Antonio data should not be stored on portable computing devices. In the event that there is no alternative to local storage, such data must be encrypted using University-approved encryption techniques. Assistance with protecting or encrypting information is available by contacting the ITS Help Desk.

2.3. Remote access to A&M-San Antonio systems must utilize approved techniques when transmitting or receiving sensitive or confidential information.

2.4. Unattended portable computing devices shall be kept physically secure using means appropriate to the potential risk associated with the device. This may include storing the device in a locked office, desk drawer, or filing cabinet, or securing the device via a cable lock system.

2.5. Device and Information Resource Owners will ensure that any portable computing device within their area of responsibility is being managed and used in accordance with all applicable University acceptable use Rules and Standards.

2.6. ITS reserves the right to inspect any system or equipment connecting to the network and disconnect as necessary for business or other risk related reasons.

2.7. Users possessing portable computing devices with access to sensitive information must comply with 29.01.03.00.13 Encryption of Confidential and Sensitive Information.

2.8. The University is not responsible for the recovery or maintenance of personal content to include but not limited to music or pictures files that may be lost while the device is issued to the employee. It is the responsibility of the individual to recover any files stored on the device upon transfer or termination of employment.

2.9. Users are prohibited from using University owned portable computing devices to access inappropriate or obscene material.

2.10. ITS will provide limited support for applications or software on portable computing devices not adopted universally by the University.

2.11. Internet connectivity will be accessible on campus via the wireless network for authorized users. Some ITS applications may not be compatible or accessible through portable computing devices.

Privacy

1. Standard Statement

   Privacy policies are mechanisms used to establish the limits and expectations for the users of A&M-San Antonio information resources. The general right to privacy is extended to the electronic environment to the extent possible. Privacy is mitigated by the Texas Public Information Act, administrative review, computer system administration, and audits. Contents of electronic files will be examined or disclosed only when authorized by their owners, approved by an appropriate A&M-San Antonio official, or required by law.

2. Official Responsibilities and Standard

   2.1. Privacy of information must be provided to users of A&M-San Antonio information resources consistent with obligations of Texas and federal law and/or secure operations.

   2.2. In the normal course of their duties, custodians may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

   2.3. Electronic files created, sent, received, or stored on University-owned, leased, administered, or otherwise under the custody and control of A&M-San Antonio are not private and may be accessed by authorized employees at any time without knowledge of the Information Resource Owner or owner as required to conduct business related activities. It is the expectation that authorized employees will treat any information viewed or accessed as confidential.

2.4. To manage systems and enforce security, A&M-San Antonio may log, review, and otherwise utilize any information stored on or passing through its information systems in accordance with the provisions and safeguards provided in the TAC 202, Information Security Standards. For these same purposes, A&M-San Antonio may also capture user activity such as telephone numbers dialed and web sites visited. In the normal course of their duties, system administrators may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

2.5. In order to protect against hardware and software failures, backups of all data stored on University information resources may be made. System administrators have the right to examine the contents of these backups to gather sufficient information to diagnose and correct problems with system software, hardware, or performance. It is the user's responsibility to find out retention policies for any data of concern.

2.6. A wide variety of third-parties have entrusted their information to A&M-San Antonio for business purposes, and all workers at A&M-San Antonio must do their best to safeguard the privacy and security of this information. The most important of these third-parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.

2.7. The CEO or designee may designate certain individuals or functional areas that may monitor user activities and/or examine data solely to determine if unauthorized access to a system or data is occurring or has occurred. If files are examined, the file owner will be informed as soon as practical, subject to delay in the case of an on-going investigation.

2.8. Information resource owners or custodians will provide access to information requested by auditors in the performance of their jobs. Notification to file owners will be as directed by the auditors.

2.9. The University collects and processes many different types of information from third parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations (e.g., Gramm-Leach-Bliley Act, TAC 206).

2.10. Individuals who have special access to information because of their position have the absolute responsibility to not take advantage of that access. If information is inadvertently gained that could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

2.11. Users of A&M-San Antonio information resources shall call the ITS helpdesk or ISO to report any compromise of security which could lead to divulging confidential information including, but not limited to, posting social security and credit card numbers to the Internet.

2.12. Users shall not attempt to access any A&M-San Antonio data or systems that they do not have authorization or explicit consent from the owner or appropriate employee to access.

Security Monitoring

1. Standard Statement

   Security monitoring is one method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of system logs, firewall logs, automated intrusion detection logs, network scanning logs, application logs, data backup logs, and other log and error files.

2. Reason for Standard

   The purpose of the implementation of this Standard is to ensure that information resource security controls are in place, are effective, and are not being bypassed. One key benefit of security monitoring is the potential of early identification of wrongdoing or security vulnerability. Early identification can help minimize the potential impact to A&M-San Antonio information resources.

3. Official Responsibilities and Standard

3.1. All A&M-San Antonio computers and network activity are subject to ongoing and unannounced security audits. The inappropriate use of information resources which violates the A&M-San Antonio policies or local, state and federal laws will be investigated. The CIO will authorize these investigations and the appropriate authorities will be notified. The ISO will be responsible for conducting these audits as necessary and ensuring that the IRM remain informed of all results.

3.2. A&M-San Antonio has the right to disclose the contents of electronic files, as required by law, System Internal Audit, or System Office of General Counsel.

3.3. The ISO will be the contact for resolution of security-related anomalies or other suspicious activity.

3.4. Automated tools will provide real time notification of detected wrongdoing or vulnerability exploitation if available. These tools will be deployed to monitor Internet traffic, electronic mail traffic, and LAN traffic.

3.5. Log files and trouble tickets will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk. Those log files include automated intrusion detection logs, network scanning logs, application logs, data backup logs, and other log and error files.

3.6. Checks will be performed, at a minimum annually, for password strength, unauthorized network devices, unauthorized personal web servers, and unsecured or inappropriate sharing of devices.

3.7. Any discovery of security issues should be reported to the ISO and/or the IRM for follow-up investigation.

System Development and Acquisition

1. Standard Statement

   This Standard sets the requirements for developing and implementing new application software in the University.

2. Official Responsibilities and Standard

   2.1. For any new software application development requests or changes to existing internal applications, requests must be submitted through Information Technology Advisory Council (ITAC) and the CIO for review and approval. Systems or software that impact two or more department or qualifies for universal adoption require an ITAC recommendation.

   2.2. Upon approval, ITS is responsible for participating in system development projects. All projects should include a plan to address any applicable areas listed: preliminary analysis or feasibility study, risk identification and mitigation, systems analysis, general design, detail design, development, quality assurance and acceptance testing, implementation, and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is deployed into an A&M-San Antonio production environment.

   2.3. All production systems must have designated owners and custodians for the critical information they process. ITS must perform assessments of production systems to determine whether the controls employed are adequate.

   2.4. All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. A designated access control administrator must be assigned for all production systems.

   2.5. Where resources permit, there should be a separation between the production and test environments, if applicable.

Wireless Access

1. Standard Statement

   Wireless networks provide a network connection that can be used without any physical connection within a limited area (e.g. building). Wireless networking is not intended to replace a wired connection. This Standard is a supplement to the Network Access Security.

2. Official Responsibilities and Standard

   2.1. Wireless networking is available by connecting to the applicable A&M-San Antonio SSID, opening a browser, and navigating to http://www.tamusa.tamus.edu if you are not automatically redirected there. Valid credentials are required in order to sign on and receive wireless access.

   2.2. Wireless access must be password protected and access must be linked to an individual through authentication mechanisms.

   2.3. If confidential and/or sensitive information is accessed through the wireless network, then that information must be encrypted as defined in 29.01.03.00.13 Encryption of Confidential and Sensitive Information.

   2.4. Information resources security controls must not be bypassed or disabled unless reviewed and approved by the Information Resources Manager (IRM) or delegated ISO.

   2.5. ITS will monitor for unauthorized wireless access points. Any unauthorized access point detected on the A&M-San Antonio network will be disconnected from the network and a security incident will be filed by the ISO per Standard 29.01.03.00.08 Incident Management.

   2.6. Only approved wireless clients are allowed to access the A&M-San Antonio wireless network.

2.7. The manufacturer default settings of the Service Set Identifier (SSID) must be changed upon initial configuration of any wireless access device. All default passwords must also be disabled or changed.

Password Authentication

1. Standard Statement

   This Standard establishes measures to mitigate information security risks associated with password and authentication issues.

2. Reason for Standard

   2.1. User authentication is a means to control who has access to information resources. The confidentiality, integrity, and availability of information can be lost when access is gained by a non-authorized entity. This, in turn, may result in loss of revenue, liability, erosion of trust, embarrassment, or damage to the University's reputation.

   2.2. There are several ways to authenticate a user, including:

      2.2.1. Something you know – password, Personal Identification Number (PIN);

      2.2.2. Something you have – Smartcard;

      2.2.3. Something you are – fingerprint, iris scan, voice;

      2.2.4. A combination of the above factors – Smartcard and a PIN;

3. Official Standard

   3.1. Applicability

      3.1.1. This Standard is intended to apply to all University information resources and those employees, students, guest and/or visitors that use these resources.

3.1.2. The Information Resource Owner or designee is responsible for ensuring that the risk mitigation measures described in the Standard are implemented. Based on risk management considerations and business function, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this Standard. Such risk management decision should be documented and made in consultation with the designated ISO.

3.2. Process

All passwords shall be constructed and implemented according to the following criteria:

3.2.1. Information resources that are mission critical and/or maintain confidential information shall have passwords that conform to this Standard.

3.2.2. Passwords must be treated as confidential information. Passwords may only be revealed to University information resources personnel such as university computer technicians only if such information is absolutely necessary to conduct maintenance on an information resource.

3.2.3. Passwords with elevated permissions will not be used for day-to-day use.

3.2.4. Passwords shall be routinely changed (no longer than 90 day intervals for systems processing/storing mission critical and/or confidential data).

3.2.5. Passwords embedded in programs intended for machine-to-machine interaction (e.g., backups, stored Standards) are not subject to the routine change specified. Instead, owners of systems shall document a separate risk management process for each password. This process must include a compensating control (e.g., an account audit) that ensures a compromised password will not go undetected.

3.2.6. Where feasible, owners of systems that maintain mission critical and/or confidential information shall not be allowed to reuse the last five (5) passwords. For systems that cannot be configured to meet this criteria, the owner of the system shall establish a reasonable period of time for passwords to be maintained in history to prevent their reuse.

3.2.7. Passwords should not be anything that can be easily associated with the account owner such as: University name or mascot, user name, social security number, UIN, nickname, relative's name, birth date, telephone number, etc.

3.2.8. Passwords should not be dictionary words or acronyms regardless of language of origin.

3.2.9. Stored passwords shall be encrypted.

3.2.10. There shall be no more than five tries before a user is locked out of an account. Delay, or progressive delay, helps to prevent automated "trial-and- error" attacks on passwords.

3.2.11. Changes to access must be reported immediately to the University ISO or ITS Management when there has been a change in job duties which no longer require restricted access, or upon termination of employment.

3.2.12. If the security of a password is in doubt, the password should be changed immediately. If the password has been compromised, the event shall also be reported to the appropriate system administrator(s) and the designated ISO.

3.2.13. Discretion should be used when circumventing password entry with auto logon, application remembering, embedded scripts, or hard-coded passwords in client software for systems that process/store mission critical and/or confidential data. Users should always consider entering "no" when asked to have a password "remembered" for University information resources.

3.2.14. Computing devices shall not be left unattended in unsecured areas without enabling a password-protected screensaver or logging off device.

3.2.15. Forgotten passwords shall be reset, not reissued.

3.2.16. Self-service password reset shall be used when available. When self- service password reset is not available, support staff shall use the following Standard to set and change other users' passwords. The Standards include the following:

3.2.16.1. The user must verify his/her identity before the password is changed;

3.2.16.2. The password must be changed to a "strong" password – (see section 3 below of Password Guidelines); and

3.2.16.3. The user will be required to change password at first log on – where applicable.

3.2.17. Where possible, passwords that are user selected shall be checked by a password audit system that adheres to the established criteria of the system or service.

3.2.17.1. Automated password generation programs must use non-predictable methods of generation.

3.2.17.2. Systems that auto-generate passwords for initial account establishment must force a password change upon entry into the system.

3.2.18. Password management and automated password generation must have the capability to maintain auditable transaction logs containing information such as:

3.2.18.1. Time and date of password change, expiration, administrative reset;

3.2.18.2. Type of action performed; and

3.2.18.3. Source system (e.g., IP and/or MAC address) that originated the change request.

VENDOR ACCESS

1. Standard Statement

   Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors might have the capability to remotely view, copy, and modify data and audit logs. They might remotely correct software and operating systems problems; monitor and fine tune system performance; monitor hardware performance and errors; modify environmental systems; and, reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of liability, embarrassment, and loss of revenue and/or loss of trust to the University.

2. Reason for Standard

   2.1. This Standard applies to any university owned or operated information resource being accessed or managed by any vendor. This Standard supplements System Regulation 29.01.03 Information Security.

   2.2. The Standard applies to all departments, administrators, and vendors who are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, operations, monitoring and troubleshooting purposes. These Standards apply to remote vendor access to systems, applications, or storage media containing university sensitive information over any type of medium. These Standards also apply to direct vendor access to systems, applications, or storage media containing university sensitive information whether located on information resources owned and operated by the university or the vendor.

3. Responsibilities

3.1. The Information Resource Owners must be informed of and may deny any vendor access to information resources containing sensitive information before vendor access is granted. Requests may require a risk assessment dependent upon the system and nature of the request. Any necessary risk assessments are to be performed by the ISO or designee.

3.2. Personnel who provide vendors access to university mission critical or confidential information resources shall obtain formal acknowledgement from the vendor of their responsibility to comply with all applicable University policies, rules, procedures, standards and agreements, including but not limited to: safety, privacy, security, auditing, software licensing, acceptable use, and nondisclosure as required by the providing entity.

3.3. University employees who are procuring the services of vendors who are given access to mission critical and/or confidential information resources are expected to define the following with the vendor:

3.3.1. The university information to which the vendor should have access;

3.3.2. How university information is to be protected by the vendor;

3.3.3. Acceptable methods for the return, destruction, or disposal of university information in the vendor's possession at the end of the contract;

3.3.4. That use of University information and information resources are only for the purpose of the business agreement; any other university information acquired by the vendor in the course of the contract cannot be used for the vendors' own purposes or divulged to others;

3.3.5. Vendors shall comply with terms of applicable non-disclosure agreements;

3.3.6. Ownership of any upgrades, modifications, patches, downloads, websites, website information, operating systems, source code and data.

3.4. The University shall provide an information resources point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with university policies and procedures.

3.5. Each vendor shall provide the information resources point of contact and notify the University of all employees assigned to university contracts. This information may be provided through an initial list of assigned employees and/or electronic communications to the University of any and all access changes. Vendors are to provide the University point of contact this information within 24 hours of staff changes.

3.6. Appropriate access authorization for each on-site vendor's employee shall be specified by the resource owner according to the criticality of the information resource. Where applicable, the university-issued identification or access privileges may be required and all requirements associated with issue and return of the identification must be followed.

3.7. Vendor personnel shall report all security incidents directly to appropriate university personnel that will, in return, follow the applicable University procedures regarding Incident Response.

3.8. The responsibilities and details of any vendor management involvement in university security incident management shall be specified in the contract.

3.9. The vendor must follow all applicable university change control processes and procedures. Regular work hours and duties shall be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate university management.

3.10. Upon termination of contract or at the request of the university, the vendor shall return or destroy all university information and provide written certification of that return or destruction within 24 hours. Destruction of university information shall follow the guidelines set forth by the TAC Rule 202.78 Removal of Data from Data Processing Equipment.

3.11. Upon termination of contract or at the request of the university, the vendor must immediately surrender all university identification badges, access cards, keys, software, equipment, supplies and all university owned information as defined in section 3.6. Equipment and/or supplies to be retained by the vendor must be documented by the providing entity.

Non-Compliance

Violation of this Standard may result in disciplinary action, including termination of employment for full and part-time employees; a termination of the contractual relationship in the case of contractors or consultants; dismissal for interns and volunteers; or, in the case of students, sanctions under the Student Code of Conduct, including suspension, dismissal, or expulsion.

Violation may also result in loss of access and privileges to University information resources and subject the violator to civil or criminal prosecution. The ISO has authority to de-activate, disconnect, and seize information resources that violate this Standard.

Definitions

Account – A logical construct that grants a user access to specific information resources. An account typically comprises an *identifier* (aka username, user ID, login ID), one or more *authenticators* (e.g., password, token) and any number of *permissions* (i.e., the ability to read or write specific data).

Application Custodian – The guardian or caretaker of the application; the person(s) charged with implementing the controls specified by the owner of the application. This custodian is responsible for any errors or application updates. Application custodians are responsible for testing the functionality of the application after any major change performed by either the application custodian or system custodian.

Change – Any implementation of new functionality, any interruption of service, any

repair of existing functionality, and/or any removal of existing functionality.

Change Management – The process of controlling modifications to hardware, software, firmware, and documentation to ensure that information resources are protected against improper modification before, during and after system implementation.

Confidential Information - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

Custodian - Guardian or caretaker (the holder of data). The agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

DMZ (Demilitarized Zone) - An area, a physical or logical sub-network where external facing services reside and are accessible to an untrusted network such as the Internet. Also known as a perimeter network.

Emergency Change – When an immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Encryption - The conversion of plaintext information into a code or cipher-text using a variable, called a “key” and processing those items through a fixed algorithm to create the encrypted text that conceals the data’s original meaning.

External Storage Media - Portable devices that are not permanently fixed inside a computer and are used to store data. These include, but are not limited to, USB thumb drives, CDs, DVDs, external hard drives, memory cards, etc.

Incident - Assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing, disruption or denial of service, altered or destroyed input, processing, storage, or output of information, or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Incident Report – A formal reporting of a known information technology related incident. This is performed by completing the associated ITS form.

Information Resource (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resources Manager (IRM) - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.

Information Security Office (ISO) - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

Information Technology Services (ITS) – The designated name for the central information technology department for the university.

Internet - A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies and colleges.

Intranet - A private network for communications and sharing of information similar to the Internet, but accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.

Logon ID - A unique account name that is required as the first step in logging into a secure information resource. A logon ID typically must be associated with a user password to obtain access to the information resource.

Malicious code – Software code that infects information resource and allows them to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user's information systems. Examples of such software include:

- Viruses - Pieces of code that attach to host programs and propagate when an infected program is executed.
- Worms - Particular to networked computers to carry out pre-programmed attacks that jump across the network.
- Trojan Horses - Hide malicious code inside a host program that appears to do something useful.

- Attack scripts - These may be written in common languages such as Java or ActiveX to exploit weaknesses in programs; usually intended to cross network platforms.
- Spyware - Software planted on your system to capture and reveal information to someone outside your system. It can do such things as capture keystrokes while typing passwords, read and track e-mail, record the sites visited, pass along credit card numbers, and so on. It can be planted by Trojan horses or viruses, installed as part of freeware or shareware programs that are downloaded and executed, installed by an employer to track computer usage, or even planted by advertising agencies to assist in feeding you targeted ads.

Mission Critical Information - Information that is defined by A&M-San Antonio or Information Resource Owner to be essential to the continued performance of the mission of A&M-San Antonio or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of A&M-San Antonio or department.

Network Scanning - The process of transmitting data through a network to elicit responses in order to determine configuration state or the presence of security vulnerabilities within an information system.

Owner - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

Patch - A fix or repair to a program that eliminates a known system vulnerability.

Portable Computing Device - Any device that is easily portable and is capable of receiving, transmitting, processing, and/or storing data, and that can connect by cable, telephone wire, wireless transmission or via any Internet connection to the University infrastructure and/or data systems. These include, but are not limited to, notebook computers, handheld computers, PDA's, pagers, cellphones, and portable storage devices (such as flash drives, memory cards, USBconnected storage devices, etc.)

Production System - The hardware, software, physical, procedural and organizational

issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

Sanitize - means to overwrite data on a storage device with a program that complies with Department of Defense standard 5220.22-M.

Scheduled Change – A system modification accompanied by a formal notification received, reviewed, and approved by the review process in advance of the change being made.

SSID - Service Set Identifier is the name of a wireless local area network (LAN). All wireless devices on a wireless LAN must employ the same SSID in order to communicate with each other.

System Custodian – Guardian or caretaker of the operating system and physical hardware; the person(s) charged with implementing the controls specified by the owner of the system. This custodian is responsible for operating system updates and assisting the Application Custodian with any testing or major changes to the system.

Test Environment – A testing environment is a setup of software and hardware on which testing is performed to verify functionality of newly built systems or software.

Unscheduled Change – A system modification that fails to present notification to the formal process in advance of the change being made.

User - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner's procedures and rules.

Vulnerability - A weakness or flaw in system security design, implementation, procedures or controls that can cause a violation of the system's security policy or a security breach if exploited by an attacker.

Related Authorities

System Policy 07.01 *Ethics*

System Policy 29.01 *Information Resources*

System Regulation 29.01.01 *Information Resources Governance*

A&M-San Antonio Procedure 29.01.03.O0.01 *Information Security*

A&M-San Antonio Procedure 29.01.03.O0.01.S1 Information Security Responsibilities of Users

Family Educational Rights and Privacy Act (FERPA)

Gramm Leach Bliley Act (GLB Act)

Health Insurance Portability and Accountability Act (HIPAA)

Texas Administrative Code (TAC) 202 as amended or supplemented

CONTACT OFFICE

Business Affairs, Information Technology Services (210) 784-4357 (HELP)