Procedure Statement

Texas A&M University-San Antonio (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.

Reason for Procedure

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

The purpose of this Procedure is to provide a set of measures that will mitigate information security risks associated with Account Management. There may also be other or additional measures that owners of information resources, department or division heads will provide to further mitigate risks. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this Procedure based on documented and approved information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

Official Responsibilities and Procedure

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. 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.

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

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

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.

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.

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.

4. Passwords associated with Logon IDs shall comply with the university system password management Procedure.

Non-Compliance

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to the University information resources, civil, and/or criminal prosecution.

Related Rules

DIR Practices for Protecting Information Resources Assets

Family Educational Rights and Privacy Act (FERPA)
Gramm Leach Bliley Act (GLB Act)

Health Insurance Portability and Accountability Act (HIPAA)

TAMU System Policy 29.01 Information Resources

Texas Administrative Code (TAC) 202 as amended or supplemented

Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education

Definitions

Accounts - Information Resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

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.

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.

Information Resources (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 Officer (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.

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.

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.

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.

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.

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.

Contact Office

Finance and Administration, Information Technology Services (210)784-4357 (HELP)