29.01.03.H0.01 Account Management

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

University information resources are strategic assets which, being property of the State of Texas, must be managed as valuable state resources. Access to University information resources is normally controlled by a logon ID associated with an authorized account. Proper administration of these logon IDs is very important to ensure the security of confidential information and the normal business operation of University managed and administered information resources.

Reason for Regulation

- Required by Texas Administrative Code Section 202
- This Standard Administrative Procedure (SAP) applies to University information resources that store or process mission critical and/or confidential information.
- The purpose of the implementation of this SAP 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 will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. 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 SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer (ISO).
- The intended audience for this standard administrative procedure includes, but is not limited to, all information resources data/owners, users, management personnel, students and system administrators.

Procedures and Responsibilities

An approval process is required prior to granting access authorization for 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.

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 when used to access mission critical and/or confidential information.

1. Account creation processes are required to ensure that only authorized individuals receive access to information resources.
2. Processes are required to disable logon IDs that are associated with individuals that are no longer employed by, or associated with, the University.
3. In the event that the access privilege is to remain active, the department (e.g., owner, department head) shall document that a benefit to the University exists.
4. All new logon IDs that have not been accessed within a period of six months from the date of creation will be disabled.
5. All logon IDs having access to mission critical and/or confidential resources that have not been used/accessed within a period of six months, shall be disabled. Exceptions can be made where there is an established departmental procedure. These actions shall be reviewed and approved by the department head or director. Documentation shall be maintained by the system administrator or other designated responsible university official.
6. Passwords associated with logon IDs shall comply with the University Standard Administrative Procedure for Identification and Authentication, 29.01.03.H0.11.
7. System Administrators or other designated staff:
   7.1. Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to Texas A&M University-Texarkana information resources.
   7.2. Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
   7.3. Shall have a documented process for periodically reviewing existing accounts for validity.
8. The university may also impose disciplinary measures.

Related Statutes, Policies, or Requirements

- Texas Administrative Code Section 202

Definitions

Account: information resource users are typically assigned logon credentials which include, at the minimum, a unique user name and password.

Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act.

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 Security Officer (ISO): responsible for administering the information security functions within Texas A&M University-Texarkana and reports to the Information Resources Manager (IRM).

Logon ID: a user name that is required as the first step in logging into a secure system. Generally, a logon ID must be associated with a password to be of any use.

Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University 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 the University or department.

Owner of an Information Resource: an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Contact Office

Contact Office: Department of Information Technology, 903-223-3084