SAP 29.01.03.T0.02 Information Technology Services – Account Management

Approved:	May 4, 2006
Revised:	February 5, 2012
Reviewed:	July 1, 2014
Next Scheduled Review:	July 1, 2019

Procedure Statement

Tarleton State University's (Tarleton) information resources are strategic assets which, as 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 Procedure

This Standard Administrative Procedure (SAP) applies to university information resources that store or process mission critical and/or confidential information. The purpose of this SAP is to provide a set of measures that will mitigate information security risks associated with account management. There may 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 will 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. The intended audience for this SAP includes, but is not limited to, all information resources data/owners, management personnel, 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 will have a unique logon ID and associated account for accountability purposes.

Role accounts (e.g., guest or visitor) will 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 who 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. Passwords associated with logon IDs shall comply with the university SAP 29.10.03.T1.10, Password Authentication.

5. System administrators or other designated staff:
   a) Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to Tarleton information resources.
   b) Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
   c) Shall have a documented process for periodically reviewing existing accounts for validity.

Related Statutes, Policies, or Requirements

Tarleton SAP *29.01.03.T0.19, Security of Electronic Information Resources*
Tarleton SAP *29.01.03.T0.10, Password Authentication*

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 the university 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 a department or the university.

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

Information Technology Services
Executive Director and CIO of Information Technology Services
254.968-9395