Texas A&M University System Standard - Account Management

Standard Statement

This standard provides procedures for the secure management of access authorization and associated credentials (e.g., User ID and password) for information technology resources.

Definitions

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. Refer to the Data Classification Standard contained in TAMUS Regulation 29.01.03.

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

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.

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 System Offices (SO) or information resource owner to be essential to the continued performance of the mission of the SO. 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, and failure to comply with regulations or legal obligations, or closure of the department.

Owner of an Information Resource - an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Standard and Responsibilities

1. GENERAL

SO information resources are strategic assets which, being property of the State of Texas, must be managed as valuable state resources. Access to SO 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 normal business operation of SO managed and administered information resources.

2. APPLICABILITY

This Standard Administrative Procedure (standard) applies to SO information resources that store or process mission critical and/or confidential information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The intended audience for this standard administrative procedure includes, but is not limited to, all information resources data/owners, management personnel, and system administrators.

3. STANDARDS

3.1 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 (see SO Rule 29.01.99.S2 Rules for Responsible Computing) and the granting of authorization by the resource owner or their designee.

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

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

3.4 Account creation processes are required to ensure that only authorized individuals receive access to information resources.

3.5 Processes are required to disable logon IDs that are associated with individuals that are no longer employed by, or associated with, the SO. 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 SO exists.

3.6 All new logon IDs that have not been accessed within a reasonable period of time from the date of creation will be disabled.

3.7 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 official.

3.8 Passwords associated with logon IDs shall comply with SO standard for *Password/Authentication*.

3.9 System Administrators or other designated staff:

3.9.1 Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to SO information resource.

3.9.2 Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.

3.9.3 Shall have a documented process for periodically reviewing existing accounts for validity.

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer