The Division of Information Technology
University Information Security Standards

Information Security Standard – Account Management (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

West Texas A&M University information resources are strategic assets, which being property of the State of Texas, must be managed as valuable state resources. Computer accounts are the means used to grant access to West Texas A&M University information resources. These accounts provide a means of providing accountability, a key to any computer security program, for information resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program. The purpose of the West Texas A&M University account management security policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

2. Applicability

This standard applies to all University information resources.

The purpose of this standard 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 department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. 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 is based on documented and approved information security risk management decisions and business functions.

The West Texas A&M University account management security policy applies equally to all individuals with authorized access to any West Texas A&M University Information Resources.

3. Definitions

3.1 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.

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

3.3 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.

3.4 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.

3.5 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

3.6 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

3.7 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities

involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.8 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

4. Procedures

4.1 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.

4.2 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.

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

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

4.3.2 Processes are required to disable logon IDs that are associated with individuals that are no longer employed by, or associated with the University. 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.

4.3.3 All access to information resources must be reviewed at least bi-annually and documented as such.

4.3.4 All logon IDs having access to mission critical and/or confidential resources that have not been used/accessed within a period of six

months, shall be disabled. Exceptions can be made where there is an established departmental procedure.

4.4 Passwords associated with logon IDs shall comply with the university system password management standards.

4.5 Information Security Administrators or other designated staff:

4.5.1 Shall have a documented process for removing the accounts of individuals who are no longer authorized to have access to university information resources.

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

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

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer