# The Division of Information Technology
# University Information Security Standards

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

## 1. General

Information Technology Division support staff, information security administrators, system administrators and others may have special access account privilege requirements compared to the access privileges of typical users. Administrator accounts and other special access accounts have extended and overarching privileges in comparison with typical user accounts, thus the granting, controlling and monitoring of these accounts is extremely important to an overall security program. The purpose of the University Administrator/Special Access Management procedure is to establish the process for the creation, use, monitoring, control and removal of accounts with special access privilege.

## 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 Administrator's Special Access. 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 intended audience includes, but is not limited to, all information resources data/owners, management personnel, system administrators, and end-users. All university faculty and staff responsible for information resources.

## 3. Definitions

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 User Data: User-generated electronic forms of information that may be found in the content of a message, document, file, or other form of electronically stored or transmitted information.

3.7 Vendor: Someone who exchanges goods or services for money.

3.8 Descriptive Data Information: Information created by a computer system or information resource that is electronically captured and which relates to the operation of the system and/or movement of files, regardless of format, across or between a computer system or systems. Examples of captures information are dates, times, file size, and locations sent to and from.

**4. Procedure**

4.1 West Texas A&M departments shall maintain a list(s) of personnel who have administrator, or special access accounts for departmental information resources systems. The list(s) shall be reviewed at least annually by the appropriate division/department head, director, or their designee.

4.2 All users of administrator or special access accounts must have account management instructions, training, and authorization.

4.3 Each account used for administrative/special access must meet the password policy.

4.4 Each individual that uses administrator/special access accounts will refrain from abuse of privilege and shall only conduct investigations as directed by appropriate university management personnel (i.e., university administrators; division/department heads or directors; or, information technology personnel.

4.5 In those cases where law enforcement agencies request access in conjunction with an investigation, the request shall be in writing (e.g., subpoena, court order). All such requests shall be reported to the appropriate division/department head, director, or their designee before any action is taken.

4.6 Each individual that uses administrator/special access accounts shall use the account or access privilege most appropriate for the requirements of the work being performed (e.g., user account vs. administrator account).

4.7 The password for a shared administrator/special access account shall change under the following conditions:

(1) an individual knowing the password leaves the university or department;

(2) job duties change such that the individual no longer performs functions requiring administrator/special access; and,

(3) a contractor or vendor with such access leaves or completes their work

4.8 In the case where a system has only one administrator, there must be a password stored in a secure space (safe or vault) in an envelope such that an appropriate individual other than the administrator can gain access to the administrator account in an emergency situation.

4.9 When special access accounts are developed for internal or external audits, software development, software installation, or other defined needs, they must be:

(1) Authorized by a department head;
(2) Created with a specific expiration date; and,
(3) Removed when the task or project is complete.

**OFFICE OF RESPONSIBILITY:** Information Technology

**CONTACT:** Chief Information Officer