Procedure Statement

Technical support staff, security administrators, system administrators, and others may have special access account privilege requirements compared to typical users. Administrator accounts and other special access accounts have extended and overarching privileges in comparison with typical users. Thus, the granting, controlling, and monitoring of these accounts is extremely important to an overall security program. The purpose of the university administrator access management procedure is to establish the process for the creation, use, monitoring, control, and removal of accounts with special access privilege.

Reason for Procedure

This Procedure applies to all users of Texas A&M University – San Antonio (“The University”) information resources.

The purpose of this Procedure is to provide a set of measures that will mitigate information security risks associated with Administrator Access. There may also be other or additional measures that owners of information resources, department or division heads will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be identified by the University ISO in collaboration with the Information Resource Manager, Information Resource owners, and/or department heads. 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 Procedure based on information security risk management decisions and business functions with documented acceptance of identified risk(s), notice to, and acknowledgment by the University ISO (e.g. copy of documentation provided to ISO). Such risk management decisions must be documented in the annual security assessment report.

Responsibilities

1. All Department Heads and Information Resource Owners shall maintain a list(s) of personnel who have administrator access accounts for hosted or local departmental
information resources systems. The list(s) shall be reviewed with the University ISO at least annually by the appropriate division/department head, director, or their designee.

2. In the course of normal duties, employees with administrator access privileges may access descriptive data to review various events related to the performance or security of those resources. Authorized Information Technology Services personnel may also routinely review events related to the performance and secure operation of the TAMU-SA network. System Administrators may at times also access user data in maintaining the operational integrity and security of information resources. System Administrators shall, however, maintain the confidentiality of user data to the extent possible and not divulge user data except to authorized University officials (such as described in 3.1).

3. Use of administrator access privileges to conduct personnel related investigations shall be directed by:

   3.1. Appropriate University and TAMU System management personnel (e.g. Dean, Vice President, President, System Internal Audit, Office of General Counsel)

4. Activities conducted beyond the normal routines outlined in Item 2 above (Responsibilities) involving user data shall insure that any user data is revealed only to third parties as outlined in Item 3 (Responsibilities). Compliance with all the requirements of privacy laws is required (e.g. Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, and the Texas Public Information Act).

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, or their designee upon receipt and the TAMUS Office of General Counsel.

6. Each individual that uses administrator 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).

7. All users who need local administrator access to workstations must complete the process for establishing administrative privileges (see form "Administrative Privileges for Workstation MOU").

8. Each account used for administrative access must follow requirements established in SAP 29.01.03.O0.25 "Password Authentication".

9. Each individual that uses administrator access accounts will refrain from abuse of privilege and shall only conduct reviews as directed by appropriate university management personnel or Information Resource Manager (IRM).

10. The password for a shared administrator access account shall change under the following conditions:

    10.1. An individual knowing the password leaves the university or department;
10.2. Job duties change such that the individual no longer performs functions requiring administrator access;

10.3. A contractor or vendor with such access leaves or completes their work;

10.4. Shared administrator passwords will be changed a minimum of every six (6) months if a previously listed event does not trigger a prior password change.

11. 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.

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

12.1. Authorized by a department head;

12.2. Created with a specific expiration date; and,

12.3. Removed when the task or project is complete.

Related Policy and Procedures

07.01 Ethics Policy
29.01.03.O0.02 Acceptable Use for Information Technology
29.01.00.O0.25 Password Authentication

Forms

Administrative Privileges for Workstation MOU

Definitions

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 Resources Manager (IRM) – The IRM ensures that all information resources are acquired appropriately, implemented effectively, and complies with
regulations and agency policies. Per requirements of the State of Texas, each agency or institution of higher education must designate an IRM.

**Information Resource Owner** – an entity responsible for:
- A business function; and,
- Determining controls and access to information resources supporting that business function.

**Information Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The ISO is the university’s internal and external point of contact for all information security matters.

**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.

**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.

**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.

**Vendor** - Someone who exchanges goods or services for money.

**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.

---

**Contact Office**

Finance & Administration, Information Technology Services – (210) 784-4357 (HELP)