Texas A&M University System Standard - Administrator/Special Access

Standard Statement

This standard provides for the appropriate management of the creation, use, monitoring, control, and removal of accounts with special access privileges (e.g., system administrator accounts).

Definitions

Descriptive data (e.g., logs) - 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 captured information are dates, times, file size, and locations sent to and from.

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.

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.

Information Resource Owner - an entity responsible for:

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

Responsibilities

1. GENERAL

   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 System Offices (SO) 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 information resources managed by the SO.

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 is all SO staff responsible for information resources.

3. STANDARDS

3.1 SO 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 department head, director, or their designee.

3.2 In the course of their normal duties to assure the availability, integrity, utility, authenticity, and confidentiality of IT resources, administrators with special access privileges may routinely access descriptive data to investigate various events related to the performance or security of those resources. 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 SO officials (such as described in 3.3).

3.3 Use of special access privileges to conduct investigations related to user data shall be directed by:

3.3.1 Appropriate SO management personnel (e.g., Department Head, Director, Vice Chancellor, etc.);

3.3.2 SO officials conducting investigations (e.g., System Internal Audit, Office of General Council, Designated Officer conducting inquiry investigating possible misconduct in research or scholarship, Investigating Authority in a sexual harassment investigation, investigation of Student Rules violations, or TAMUS CIO.

Prior to conducting such investigations, the individual with administrator/special access will consult with TAMUS CIO

3.4 Investigations conducted beyond the normal routines outlined in 3.2 and involving user data shall insure that any user data is revealed only to disinterested

third parties as outlined in 3.3 and all the requirements of privacy laws are maintained (e.g., Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, and the Texas Public Information Act).

3.5 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 department head, director, or their designee upon receipt and the Texas A&M System Office of General Counsel.

3.6 Each individual who 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).

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

3.7.1 An individual knowing the password leaves the SO department;

3.7.2 Job duties change such that the individual no longer performs functions requiring administrator/special access; and,

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

3.8 In the case where a system has only one administrator, there shall be a password escrow procedure in place such that an appropriate individual other than the administrator can gain access to the administrator account in an emergency situation.

3.9 When special access accounts are needed for internal or external audit, software development, software installation, or other defined need, the need must be:
3.9.1 Authorized;
3.9.2 Created with a specific expiration date; and,
3.9.3 Removed when the work is complete.

3.10 Passwords for special administer passwords should be of maximum strength. Where possible the should be at least 16 characters in length, contain no dictionary words, contain no repeating or sequential characters, and contain a mix of upper and lower case letters, numbers, and other symbols

Contact Office

Contact The Texas A&M University System Chief Information Officer for standard interpretation or clarification.

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