Information Resources – Administrator/Special Access Management

Approved January 20, 2004
Revised November 21, 2006
Revised September 15, 2009
Revised June 5, 2013
Next Scheduled Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
The scope of this procedure is to allow special access account privilege.

Reason for Standard Administrative Procedure
The purpose of the administrator/special access management procedure is to establish the process for the creation, use, monitoring, control and removal of accounts with special access privilege.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

1.1 Divisions shall maintain a list(s) of personnel who have administrator, or special access accounts for division information resources systems. The list(s) shall be reviewed at least annually by the appropriate division head, director, or their designee.

1.2 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 TEES officials (such as described in 1.3).

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

1.3.1 Appropriate TEES management personnel (e.g., Division Head, Director, etc.);

1.3.2 University officials conducting investigations (e.g., System Internal Audit, Office of General Counsel, Designated Officer conducting
inquiry investigating possible misconduct in research or scholarship, Investigating Authority in a sexual harassment investigation, investigation of Student Rules violations, or representatives of Security Monitoring Team (SMT), etc.). Prior to conducting such investigations, the individual with administrator/special access will consult with SMT.

1.4 Investigations conducted beyond the normal routines outlined in 1.2 and involving user data shall insure that any user data is revealed only to disinterested third parties as outlined in 1.3 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).

1.5 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 head, director, or their designee upon receipt and the System Office of General Counsel.

1.6 Each individual that uses administrator/special access accounts shall use the account or access privilege most appropriate with work being performed (i.e., user account vs. administrator account).

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

1.7.1 an individual knowing the password leaves the TEES division;

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

1.7.3 a contractor or vendor with such access leaves or completes their work.

1.8 In the case where a system has only one administrator there shall be a password escrow procedure in place so that their division head or their designee can gain access to the administrator account in an emergency situation.

1.9 When special access accounts are needed for internal or external audit, software development, software installation, or other defined need, the need must be:

1.9.1 authorized;

1.9.2 created with a specific expiration date; and,

1.9.3 removed when the work is complete.
Related Statutes, Policies, or Requirements
Family Educational Rights and Privacy Act

Health Insurance Portability and Accountability Act

TAMU SAP 29.01.99.E1.04, Information Resources – Administrator/Special Access

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

Texas Public Information Act

Contact Office
Information Technology Services
(979) 847-8585