29.01.03.H0.03 Administrative/Special Access

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important for an overall security program.

Reason for Procedure

The purpose of this procedure is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege. It applies to all individuals who have, or may require, special access privilege to any Texas A&M University-Texarkana (TAMUT) Information Resource.

Definitions

Abuse of Privilege: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, 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, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes 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.

Information Security Officer (ISO): Person responsible to the executive management for administering the information security functions within the University. The ISO is TAMUT's internal and external point of contact for all information security matters.

NetID: Single sign on credential for most University systems.

Information Technology: The name of the University department responsible for computers, networking and data management.

System Administrator: Person responsible for the effective operation and maintenance of IR, including implementation of standard procedures and controls, to enforce an organization's security policy.

Procedures and Responsibilities

1. ADMINISTRATIVE/ SPECIAL ACCESS

1.1 University departments must submit (to INFORMATION TECHNOLOGY) a list of computer administrator contacts for their systems that are connected to the TAMUT network.

1.2 All users must sign the Local Administrative Privileges Request Form before administrative access is given to an account.

1.3 Administrative/Special accounts must be renewed yearly. The request form must be re-submitted for review.

1.4 Administrative/Special accounts will be locked after 60 days of inactivity and will have 120 days to get their account unlocked by contacting our Help Desk.

1.5 Each individual who uses Administrative/Special access accounts must refrain from abuse of privilege and/or making changes to the configuration of the computers, including formatting, uninstalling University supported software, etc. See 29.01.99.H0.01 Acceptable Use Procedure.

1.6 Each individual who uses Administrative/Special access accounts must use the account privilege most appropriate for the work being performed (i.e., user account vs. administrator account). Individuals must log on with their NetID and only use the administrator account under the "run as" option.

1.7 Administrative/Special accounts that are not in compliance with this and/or other related SAPs will be disabled.

1.8 Administrative/Special accounts will be deleted upon an employee's separation, termination, or retirement, and for third parties no longer in contract with the University.

1.9 All passwords for accounts used for administrative/special access must be constructed in accordance with the Procedure 29.01.03.H0.11 Identification and Authentication.

1.10 The password for a local Administrator/Special access account must be changed when an individual with the password leaves the department or TAMUT, or upon a change in third party personnel assigned to the TAMUT contract.

1.11 When Special Access accounts are needed for internal or external audit, software development, software installation, or other defined need, requestors:

1.11.1 must submit the Local Administrative Privileges Request Form.

1.11.2 must be authorized by the dean and CIO/ISO.

1.12 Users must be made aware of the privileges granted to their accounts, especially those that impact access to information resources or that allow them to circumvent controls in order to administer the information resource.

2. MONITORING AND REVIEW

A review of special access will be completed at least annually or as determined by TAMUT's Information Security Officer. The review process will involve the following steps:

2.1 A report will be generated from Active Directory. The report will list special access by system and access type, and access by person (i.e. for each person, all access given to that person is listed).

2.2 The reports will be distributed to the Chief Information Officer, Information Security Officer and the VP or dean of users who are given special access. Each person reviews the list (or appropriate part thereof) to determine if any changes should be made.

2.3 Should anyone determine that an individual needs to be added to other special access groups, that individual must submit a Local Administrator Access Form requesting the additional access.

2.4 If there are any deletions that need to be made to the permissions, Systems Administrators will make the appropriate changes.

3. DISCIPLINARY ACTIONS

3.1 Violation of this SAP may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion for students. Additionally, individuals are subject to loss of TAMUT Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Information Security Officer, 903-886-5425