TEXAS A&M **INTERNATIONAL** UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.03 Administrative/Special Access

First Approved: November 15, 2013
Revised: June 22, 2017
Next Scheduled Review: June 22, 2022

Procedure Statement and Reason for Procedure

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.

The purpose of this SAP is to establish the process for the creation, use, monitoring, control, and removal of accounts with special access privileges. This SAP applies to all individuals who have, or may require, special access privileges to any Texas A&M International University (TAMIU) Information Resource. This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

Procedures and Responsibilities

1. Administrative/Special Access

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

    1.2 All local administrative accounts must follow TAMIU's account management procedures as outlines in *TAMIU SAP 29.01.99.L1.02, Account Management* unless otherwise noted in this SAP.

1.3 Administrative/special accounts must be renewed yearly and approved by the Chief Information Officer (CIO) and CEO.

1.4 Administrative/special accounts will be locked after sixty (60) days of inactivity. Such inactive accounts may be deleted after 120 days.

1.5 Each user with administrative/special access accounts must refrain from abuse of privilege and/or making changes to the configuration of the computers, including formatting and uninstalling TAMIU-supported software. See *TAMIU SAP 29.01.99.L1.01, Acceptable Use*.

1.6 Each user with administrative/special access accounts must use the account privilege most appropriate for the work being performed (i.e., user account vs. administrator account). Such accounts cannot be used in lieu of individuals' NetID accounts.

1.7 Administrative/special accounts that are not in compliance with this and/or other related SAP's will be disabled or deleted.

1.8 Individual administrative/special accounts will be deleted upon a user's separation, termination, or retirement, and for third parties no longer under contract with the TAMIU. Owners of departmental administrative/special accounts must have the password changed anytime a member of the department who uses said account separates, terminates, or retires.

1.9 All passwords for accounts used for administrative/special access must be constructed in accordance with the *TAMIU SAP 29.01.99.L1.13, Password Management*.

1.10 When special access accounts are needed for external entities such as System Audit, Third Party Vendors, etc., such requestors must:

a. submit a Guest Access Request **and/or**
b. submit a "Local Administrative Privileges Request" **and**
c. be authorized by the appropriate VP and CIO/ISO.

1.11 Users with administrative/special access may not use such privileges granted to other accounts, especially those that impact access to information resources, to circumvent controls in order to administer the information resource.

Related Statutes, Policies, Regulations, or Rules

Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education
TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources
TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities

Appendix

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

Office of Information Technology, 956-326-2310