TEXAS A&M INTERNATIONAL UNIVERSITY™

STANDARD ADMINISTRATIVE PROCEDURE

29.01.99.L1.02 Account Management

Approved: October 29, 2013
Last Revised: October 08, 2013
Next Scheduled Review: October 29, 2015

Standard Administrative Procedure Statement

GENERAL
Computer accounts are used to grant access to Texas A&M International University (TAMIU) Information Resources. These accounts provide a means of accountability. Creating, controlling, and monitoring all computer accounts is extremely important for an overall security program.

APPLICABILITY
The purpose of this SAP is to establish procedures for the creation, monitoring, control and removal of user accounts. It applies to all individuals with authorized access to TAMIU Information Resources.

Definitions

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.

NetID: Single sign on credential for most University systems.

Standard Operating Procedure (SOP): Set of detailed instructions for performing a specific process.

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

Procedures and Responsibilities

ACCOUNT MANAGEMENT STANDARD ADMINISTRATIVE PROCEDURE

A NetID and password are required to access TAMIU's Information Resources. New students, faculty and staff receive a NetID upon arrival to TAMIU. Questions regarding NetID information should be directed to the OIT Help Desk.

Authorization is based on the account type and departmental requirements for accessing resources. The table below lists the various TAMIU user accounts and the rights that are associated with each account.

	TAMIU.EDU Domain Account	TAMIU Email	TAMIU DustyEmail for Life	TAMIU VPN [3]	TAMIU Wi-Fi	UConnect
Current Student	X		X		X	X
Full Time Faculty	X	X		X	X	X
Adjunct Faculty [1]	X	X		X	X	X
Staff	X	X		X	X	X
Retired [2]	X	X			X	X
Ongoing Business Partner [4]*	X			X	X	
Research Partner [4]*	X			X	X	
General Public					X*	
Student Worker	X	X			X	X
Alumni	X		X		X	X

* With sponsorship

[1] Adjunct Faculty will maintain an active NetID for the entire fiscal year in which they are hired.

[2] Emeritus faculty members and alumni keep their NetID account while in good standing with the University.

[3] A VPN Access Form must be submitted and approved by the person's supervisor or sponsor.

[4] Guest Access is granted when a Guest Access Form is submitted to OIT by a faculty or staff member sponsoring the guest.

ACCOUNT MANAGEMENT

1.1 All created accounts must have an associated request and approval that is appropriate for the TAMIU system or service.

1.2 Information Resources technical support staff, security administrators, systems administrators and others with special access to the IR infrastructure must abide by the 29.01.99.L1.03 Administrative/Special Access SAP and must sign a Non-Disclosure Agreement form.

1.3 All student and staff accounts must be uniquely identifiable using the assigned username.

1.4 All passwords for accounts must be constructed in accordance with the 29.01.99.L1.13 Password SAP.

1.5 All accounts must have a password expiration that complies with the 29.01.99.L1.13 Password SAP.

1.6 System Administrator or other designated staff:

1.6.1 Must remove access to accounts and privileges of individuals who change roles within the University or who are separated from their relationship with TAMIU when identified as such by HR.

1.6.2 Must provide a list of accounts for the systems they administer when requested by authorized University management.

1.6.3 Must cooperate with authorized University management investigating security incidents.

1.6.4 Must sign a non-disclosure agreement prior to obtaining access to an account.

1.6.5 Must follow SOP for termination of accounts.

1.7 Any account that is inactive for 60 days will be disabled following the Windows Account Audit SOP.

1.8 The following procedures will be followed for exiting employees.

1.8.1 Upon request of the former employee or retiree (via the E-mail Extension Form), and with the approval of the dean and VP, said employee's e-mail account will be kept active for a period of 3 months.

1.8.2 A standard out-of-office reply will be set up stating that the employee (name) is no longer employed or has retired from Texas A&M International University but has provided the following e-mail address at which they may be reached.

1.8.3 TAMIU will not take custody of any messages coming to the employee's TAMIU.edu address.

DISCIPLINARY ACTIONS

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 TAMIU Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, Regulations, Rules or Requirement

TAC 202.75 Security Standards for Institutions of Higher Education

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
Hotline: (956) 326-2310
Killam Library 257

Office Hours
Monday - Friday: 7:30 AM - 6:00 PM
Saturday - Sunday: Closed

Information Security Officer
Cuauhtemoc Barrios
cbarrios@tamiu.edu

ITSecurity Group
itsecurity@tamiu.edu