TEXAS A&M **INTERNATIONAL** UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.11 Network Access and Security

First Approved: **March 28, 2013**
Revised: **June 22, 2017** *(replaces former TAMIU SAP's 29.01.99.L1.12, Network Configuration and 29.01.99.L1.26, Wireless Access)*
Next Scheduled Review: **June 22, 2022**

Procedure Statement and Reason for Procedure

The Information Resources network infrastructure is provided by Texas A&M International University (TAMIU) for all University departments. The network infrastructure is comprised of separate units (i.e., routers, switches, cables, wireless, software, etc.) that combine to achieve performance objectives. This is a dynamic environment where performance is impacted by multiple factors.

The purpose of this SAP is to establish the process for attaining access to and use of the network infrastructure. This SAP applies to all individuals with access to TAMIU Information Resources. 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. Network Access

   The TAMIU Office of Information Technology (OIT) is required to approve all access methods, installation of all network hardware, and methods and requirements for attachment of any computer system, device, or user to any TAMIU network. This process ensures that access to the network does not interfere with the operation and reliability of the network or impede the integrity of information contained within the network.

2. Responsibility

2.1 OIT is solely responsible for TAMIU's network infrastructure and configuration.

2.2 All new cabling will conform to state standards for cabling.

2.3 All connected network equipment must be configured to a specification approved by OIT.

2.4 All connected devices are subject to monitoring and management by OIT.

2.5 All network addressing and protocols are managed by OIT. Users are permitted to use only those network addresses issued to them by OIT.

2.6 All connection of the network infrastructure to third-party networks such as ISP or external telephone networks must be approved by OIT.

2.7 Use of departmental firewalls or other filtering devices is prohibited unless authorized by OIT.

2.8 All TAMIU entities must consult with OIT prior to the purchase/installation of any software/hardware or associated service.

3. Virus and Software Protection

3.1 All computers connecting to the TAMIU network must run authorized virus protection software that is updated with current signatures and security patches.

3.2 Virus protection software must not be disabled or bypassed except as required for the temporary installation of software or other special circumstances.

3.3 Computers infected with a virus or other malicious code will be disconnected from the TAMIU network until deemed safe by OIT.

4. Security and Network Use

4.1 Visitors must submit a "Guest Access Request" to OIT for network access approval.

4.2 Users must not alter, extend, or re-transmit network services in any way. Network aggregation devices (i.e., router, switch, hub, wireless access point) must not be connected to the TAMIU network without OIT approval.

4.3 Network management/control devices must not be connected to network infrastructure without prior consultation with OIT. Additionally, users must not alter or disable TAMIU network infrastructure devices or equipment.

4.4 Security programs, applications, or tools that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems must not be downloaded and/or used, except as authorized by OIT.

4.5 If, for any reason, a device causes any disruption to the TAMIU Information Resources network, the device will be disconnected from the network until the problem is resolved.

4.6 Users must report any weaknesses in TAMIU's computer security or any incidents of possible misuse or violation of this agreement by contacting TAMIU's Information Security Officer (ISO) at itsecurity@tamiu.edu.

4.7 If it is determined that required security software is not installed on a remote computer or that a remote computer has a virus, is vulnerable to a cyber-attack, or in some way endangers the security of TAMIU information resources, the account and/or network connection will be disabled. Access will be re-established after the computer is determined to be safe by OIT.

5. Wireless Access Procedures

5.1 TAMIU has wireless networks available to the general TAMIU community. A special limited-access wireless network is available for guest access with TAMIU-approved sponsorship. A valid TAMIU NetID is required to connect to TAMIU's private wireless networks.

5.2 Stand-alone or special utility wireless networks must be approved by the Chief Information Officer (CIO) or ISO.

5.3 Stand-alone or special utility wireless access must be protected by password or other compensating controls to ensure authorized access.

5.4 Confidential and/or sensitive information should not be accessed through the wireless network unless communication is properly encrypted (i.e., VPN, SSL, etc.)

5.5 Information resources' wireless security controls should not be bypassed or disabled.

5.6 OIT will occasionally monitor for unauthorized (rogue) wireless access points. Any rogue access point detected on the TAMIU network will be disconnected from the network.

5.7 The manufacturer default settings such as the Service Set Identifier (SSID) must be changed upon initial configuration of any wireless access device. All default passwords must also be disabled or changed.

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