29.01.99.L1.12  Network Configuration

Approval date: 03/28/13
Revision date: 01/24/13
Next scheduled review date: 01/24/15
Author: Office of Information Technology

Standard Administrative Procedure Statement

General
The Texas A&M International University (TAMIU) network infrastructure is provided as a central utility for all users. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high-speed networking technology to allow the future provision of enhanced user services.

Applicability
The purpose of this SAP is to establish the rules for the maintenance, expansion and use of the network infrastructure. These procedures are necessary to preserve the integrity, availability and confidentiality of TAMIU’s information. This SAP applies to all individuals with 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.

Information Resources Manager (IRM): Person responsible to the State of Texas for management of the agency’s information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the agency's information activities, and ensure greater visibility of such activities within and between State agencies. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards and guidelines to protect the Information...
Resources of the agency. At TAMIU, the IRM is the Associate Vice President for IT/CIO.

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

**Office of Information Technology (OIT):** The name of the TAMIU department responsible for computers, networking and data management.

### Procedures and Responsibilities

OIT is responsible for TAMIU networking infrastructure which includes all cabling, wireless signaling and connected electronic devices to ensure reliability of operations, proper accessibility to resources, and protection of data integrity. Technical aspects are reviewed by OIT’s Chief Information Officer and Information Security Officer and purchases approved by Vice President of Finance and Administration.

The Office of Information Technology is responsible for:

1. The TAMIU network infrastructure configuration; it will continue to manage further developments and enhancements to this infrastructure.
2. Operating and maintaining a reliable network with appropriate redundancies to meet quality of service goals.
3. Maintaining a list of systems connected to the TAMIU network.
4. Installing or authorizing a contractor to install all cabling and network hardware. All new or upgraded cabling will conform to state standards for cabling (Texas Administrative Code Chapter 208) to the extent consistent with TAMIU’s mission.
5. Approving the specifications used to configure all network equipment connected to the TAMIU network.
6. Authorizing changes to the configuration of active network management devices.
7. Ensuring TAMIU Firewalls are installed and configured following 29.01.99.L1.25 Firewall SAP.

User responsibilities include the following:

8. Users must not 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.
9. Users are not permitted to alter network hardware in any way.

**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 Requirements

TAC 202.75 Security Standards for Institutions of Higher Education

Appendix

References
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

<table>
<thead>
<tr>
<th>Office of Information Technology</th>
<th>Information Security Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotline: (956) 326-2310</td>
<td>Cuauhtemoc Barrios</td>
</tr>
<tr>
<td>Killam Library 257</td>
<td><a href="mailto:cbarrios@tamiu.edu">cbarrios@tamiu.edu</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Office Hours</th>
<th>ITSecurity Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
<td><a href="mailto:itsecurity@tamiu.edu">itsecurity@tamiu.edu</a></td>
</tr>
</tbody>
</table>