

**General**

The Information Resources network infrastructure is provided by Texas A&M International University (TAMIU) for all University departments. It is important that the infrastructure, which includes media, active electronic equipment (i.e. routers, switches, cables, etc.) and supporting software, is able to meet current performance requirements while retaining the flexibility to allow emerging developments in high-speed networking technology and enhanced user services.

**Applicability**

The purpose of this SAP is to establish the rules for access to and use of the network infrastructure. It 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**

Network Access

OIT is required to approve all access methods, installation of all network hardware, and methods and requirements for attachment of any computer system or device 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 use of information contained within the network.

1. **Virus and Software Protection**
   1.1 All computers connecting to the TAMIU network must run current and authorized virus protection software and must be updated with the latest software security patches.
   1.2 Virus protection software must not be disabled or bypassed except as required by the temporary installation of software or for other special circumstances.
   1.3 Computers infected with a virus or other malicious code will be disconnected from the TAMIU network until deemed safe by OIT.

2. **Security and Network Use**
   2.3 Visitors must submit a Guest Access form to OIT for network access approval.
   2.4 Users are permitted to use only those network addresses issued to them by OIT.
   2.5 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.
   2.6 Network management/control devices must not be connected to network infrastructure without prior consultation with OIT. Additionally, end-users must not alter or disable TAMIU network infrastructure devices or equipment.
   2.7 Users are not permitted to alter network hardware in any way.
   2.8 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 should not be downloaded and/or used, except as authorized by OIT.
   2.9 If for any reason a device causes any disruption to the TAMIU network, the device will be disconnected from the network until the problem is resolved.
   2.10 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 ISO at itsecurity@tamiu.edu
2.11 If it is determined that required security related software is not installed on a remote computer or that a remote computer has a virus, is party to a cyber-attack or in some way endangers the security of TAMIU, the account and/or network connection will be disabled. Access will be re-established once the computer is determined to be safe by OIT.

2.12 Currently, TAMIU’s wireless network uses only username and password as identification, and no personal profile information is needed.

2.13 Users may not use an account belonging to someone else. Users must not make copies of system configuration files for their own personal use or for other people for unauthorized uses.

2.14 OIT reserves the right to inspect the system and disconnect it from the network if necessary.

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
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
<table>
<thead>
<tr>
<th><strong>Contact Office</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office of Information Technology</strong></td>
</tr>
<tr>
<td>Hotline: (956) 326-2310</td>
</tr>
<tr>
<td>Killam Library 257</td>
</tr>
<tr>
<td><strong>Information Security Officer</strong></td>
</tr>
<tr>
<td>Cuauhtemoc Barrios</td>
</tr>
<tr>
<td><a href="mailto:cbarrios@tamiu.edu">cbarrios@tamiu.edu</a></td>
</tr>
<tr>
<td><strong>Office Hours</strong></td>
</tr>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
</tr>
<tr>
<td>Saturday - Sunday: Closed</td>
</tr>
<tr>
<td><strong>ITSecurity Group</strong></td>
</tr>
<tr>
<td><a href="mailto:itsecurity@tamiu.edu">itsecurity@tamiu.edu</a></td>
</tr>
</tbody>
</table>