General
Wireless networks provide a network connection that can be used without any physical connection within a limited area (e.g. building). It is not intended to replace a wired connection. This Standard Administrative Procedure is a supplement to the Network Access Security SAP.

Applicability
The purpose of this SAP is to establish the procedures for the access and use of the wireless network. These procedures are necessary to preserve the integrity, availability and confidentiality of Texas A&M International University (TAMIU) information and apply to all individuals with access to TAMIU Information Resources.

Definitions
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.

Service Set Identifier (SSID): The assigned name of a wireless network.

Procedures and Responsibilities

1. Wireless Access Procedures
   1.1 Wireless networking is available by connecting to the “TAMIU Unplugged” SSID, opening a browser, and navigating to http://unplugged.tamiu.edu if you are not automatically redirected there. Valid TAMIU NetID credentials are required in order to sign on and receive wireless access.

   1.2 Requests for wireless service must be provided by OIT.

   1.3 Requests for wireless service for stand-alone networks must be approved by OIT in order to prevent interference with existing wireless networks.

   1.4 Wireless access must be password protected.
1.5 Confidential and/or sensitive information must not be accessed through the wireless network unless communication is encrypted by strong encryption as determined by the ISO or using TAMIU’s VPN solution.

1.6 Information resources security controls must not be bypassed or disabled.

1.7 OIT will monitor for unauthorized wireless access points. Any rogue access point detected on the TAMIU network will be disconnected from the network and a security incident will be filed by the ISO.

1.8 The manufacturer default settings of 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, 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

### Contact Office

<table>
<thead>
<tr>
<th><strong>Office of Information Technology</strong></th>
<th><strong>Information Security Officer</strong></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><strong>Office Hours</strong></th>
<th><strong>ITSecurity Group</strong></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>
<tr>
<td>Saturday - Sunday: Closed</td>
<td></td>
</tr>
</tbody>
</table>