General
Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurances that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use and disruptions in service.

Applicability
The purpose of this SAP is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software. It applies to all individuals who are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource security.

Definitions
Office of Information Technology (OIT): The name of the TAMIU department responsible for computers, networking and data management.
Server: A computer dedicated to running one or more such services, to serve the needs of programs running on other computers on the same network.
Server Hardening: the enhancement of server security through different means, which result in a more secure server operating environment due the measures established during this process.
Vendor: Someone who exchanges goods or services for money.

Standards and Procedures
1. A server cannot be connected to the TAMIU network until it is in a University OIT approved secure state. Prior to connecting the server to the network, the following must be performed:
   a) Install the operating system from an OIT approved source which includes proper licenses.
b) Receive a reserved IP address from the campus network administrator.
c) Remove all unnecessary software, system services and drivers.
d) Set appropriate security parameters and file protections.
e) Enable audit logging.
f) Disable or change the password of default accounts.

2. Immediately after connection to the network, the following must be completed:
a) Install OIT approved antivirus software.
b) Apply the latest vendor supplied patches which have been tested for compatibility with the production environment.

3. Prior to use, all servers are required to pass a vulnerability assessment performed by OIT. Administrators are required to correct all network/operating system vulnerabilities identified as high or medium risk during the vulnerability assessment. Examples of high and medium risk vulnerabilities include:
a) Accounts with blank or weak passwords.
b) Outdated version or patch levels of server software and services.

---

**Related Statutes, Policies, Regulations, Rules or Requirements**

TAC 202.70 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Office Hours</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
</tr>
<tr>
<td>Saturday - Sunday: Closed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ITSecurity Group</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:itsecurity@tamiu.edu">itsecurity@tamiu.edu</a></td>
</tr>
</tbody>
</table>