29.01.99. L1.19 Server Hardening

Approval date:
Revision date: 03/21/11
Next scheduled review date:
Author: Office of Information Technology

Standard Administrative Procedure Statement

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.

Vendor: Someone who exchanges goods or services for money.

Procedures and Responsibilities

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.

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries, 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

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>Claudia Escobar, CISSP</td>
</tr>
<tr>
<td>Killam Library 257</td>
<td><a href="mailto:cescobar@tamiu.edu">cescobar@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>
<tr>
<td>Saturday - Sunday: Closed</td>
<td></td>
</tr>
</tbody>
</table>