CEHD Information Security Procedure
IS-10 Server Management Requirements

Procedure Statement

In compliance with the Texas Administrative Code 202, Texas A&M has established an information security program to protect the IT assets of the university (physical equipment as well as data). Protection of these assets are deemed critical to the university both in terms of their monetary value and the potential harm to the reputation of the university in the event of a security breech.

Servers are of greater importance than individual workstations because the function of a server is to provide services beyond the individual operating them. Thus, the management of a server carries additional responsibilities. This document outlines those responsibilities as defined by the CEHD.

Official Procedure and Responsibilities

It is the responsibility of IT server administrators to ensure that each server complies with state, university, and college IT security and operational policies and procedures. As such each administrator should be familiar with the A&M Rules proved at

http://cio.tamu.edu/Risk_Management_Policy/IT_Policy_Compliance/index.php

and in particular the Controls Catalog

http://cio.tamu.edu/Risk_Management_Policy/IT_Policy_Compliance/Texas_AM_IT_Policy/Information_Security_Controls_Catalog.php

Within the CEHD, a set of requirements have been developed from these rules to govern the operation of IT Servers within the college and are listed below.

1) Complete Admin rights approval process (submit Security Plan and answers to NIST questions) to be approved by Dr. Alexander

   See https://it.education.tamu.edu/it-security/administrative-authority-request-procedure for process as well as links to templates for a security plan and the NIST questions.

2) Complete with computer configuration requirements outlined in IS-6.

   https://it.education.tamu.edu/sites/it.education.tamu.edu/files/ITSecurity/IS-6%20Computer%20Configuration.pdf

3) Perform standard server hardening functions. Here is a document with suggestions https://www.sans.org/media/score/checklists/LinuxCheatsheet_2.pdf

4) Run the appropriate audit script (Linux or Windows) and provide the results to Technology Services. (Technology Services will provide this script when you are ready.)

5) Request vulnerability scan of server by Technology Services and correct any "Important" or higher vulnerabilities found.

6) Obtain a SPECTRIM account to be able to submit annual security report to university http://cio.tamu.edu/Risk_Management_Policy/IT_Risk_Management/Risk_Assessment/Assessment_Training/Assessor_SPECTRIM_Training_Schedule.php
Send request to Technology Services (Arlen Strader) to request this account on your behalf.

7) #4 and #5 will need to be repeated as part of the annual IT Risk Assessment review process each spring.

8) (Recommended) Subscribe to the AM-COMPADMIN listserv for campus administrators so you can keep up with IT happenings on campus.

Send an email to listserv@listserv.tamu.edu with the message body being

SUB AM-COMPADMIN YOUR FULL NAME

Last Update. June, 2017