The Division of Information Technology
University Information Security Standards

Information Security Standard – Platform Management (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Servers are relied upon to deliver data in a secure, reliable fashion. There must be assurance 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. Additionally, desktop computing systems must be secured and maintained to prevent similar unauthorized use and access.

2. Applicability

This information security standard applies to all University information resources that store or process mission critical and/or confidential information.

The purpose of this information security standard is to provide a set of measures that will mitigate information security risks associated with Server Hardening. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience includes, but is not limited to, system managers and administrators, who manage University information resources that store or process mission critical and/or confidential information.

3. Definitions

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

3.2 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, 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, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is 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.

3.3 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

3.4 Security Patch: a fix to a program that eliminates a vulnerability by malicious hackers.

3.5 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

4. Procedures

4.1 Information technology personnel will test security patches prior to implementation when practical. Information technology personnel are encouraged to have hardware resources available for testing security patches in the case of special applications.

4.2 System administrators shall ensure that vendor supplied security patches are routinely acquired, systematically tested, and installed promptly based on risk management decisions.

4.3 System administrators shall remove unnecessary software, system services, and drivers.

4.4 System administrators shall enable security features included in vendor supplied systems including, but not limited to, firewalls, virus scanning and malicious code protections, and other file protections (see Malicious Code standard administrative procedure). Audit logging shall also be enabled. User privileges shall be set utilizing the least privileges concept of providing the minimum amount of access required to perform job functions. The use of passwords shall be enabled in accordance with University Identification/Authentication standard administrative procedure.

4.5 System administrators shall disable or change the password of default accounts before placing the resource onto the network.

4.6 Servers, especially, shall be tested for known vulnerabilities when new vulnerabilities are announced, and shall seek and implement best practices for securing their particular system platform(s).

4.7 Altiris, GFI LanGuard, and /or Microsoft Windows Server Update Services (WSUS) shall be utilized to provide automatic hotfixes, patches, service packs, and device drivers to desktop computing systems from a centralized IT server. Additionally, information technology personnel may use other products such Microsoft Systems Management Server (SMS) to update desktop computing systems. In instances where automated update pools are unable to be utilized, manual updates will be performed as soon as reasonably possible based on risk management decisions.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer