SAP 29.01.03.T0.15 Information Technology Services – Server Hardening

Approved:	May 4, 2006
Revised:	February 28, 2012
Revised:	July 1, 2014
Next Scheduled Review:	July 1, 2019

Procedure Statement

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.

Reason for Procedure

The purpose of this Tarleton State University (Tarleton) Standard Administrative Procedure (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. In addition, this SAP provides a set of measures that will mitigate information security risks associated with server hardening. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. 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 in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated information security officer (ISO).

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

Procedures and Responsibilities

1. Departmental information technology personnel will test security patches prior to implementation (where practical). Departmental information technology personnel are encouraged to have hardware resources available for testing security patches in the case of special applications.

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

3. System administrators shall remove unused software, system services, and drivers as needed.

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 *SAP 29.01.03.T0.07, Information Technology Services-Malicious Code*). 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. Privileges may be added as need is demonstrated by the user. The use of passwords shall be enabled in accordance with *SAP 29.01.03.T0.10, Information Technology Services-Password/Authentication*.

5. System Administrators shall disable or change the password of default accounts.

6. System administrators (or their designee) shall test servers periodically for known vulnerabilities.

7. System Administrators shall seek and implement best practices for securing their particular system platform(s).

Related Statutes, Policies, or Requirements

Supplements *SAP 29.01.03.T0.19 Security of Electronic Information Resources*
References *SAP 29.01.03.T0.07, Information Technology Services-Malicious Code*
References *SAP 29.01.03.T0.10, Information Technology Services-Password/Authentication*

Definitions

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).

2. **Information Resources (IR):** the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

3. **Information Security Officer (ISO**): responsible for administering the information security functions within Tarleton and reports to the Information Resources Manager (IRM).

4. **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.

5. **Security Patch**: a fix to a program that eliminates a vulnerability exploited by malicious hackers.

Contact Office

Information Technology Services
Executive Director and CIO of Information Technology Services
254.968.9395