29.01.03.H0.21 Platform Management

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

All platforms (e.g., servers, desktop systems, notebooks, tablets, phones, and other information technology devices) 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 all platforms are initialized and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the information processed by the platform.

Reason for Procedure

The purpose of the Texas A&M University-Texarkana platform management procedure is to: describe the requirements for installing a new platform (e.g., server) in a secure fashion and for maintaining the appropriate security of the platform and application software; and provide guidance for applying and maintaining appropriate security measures for all platforms that process mission critical and/or confidential information.

The intended audience includes, but is not limited to, custodians and/or owners of an information resource.

Definitions

Confidential: Information that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements). This includes both confidential data in transit and confidential data at rest.

Examples of "Confidential" data may include, but are not limited to:

- personally identifiable information, such as a Social Security number (SSN) and/or financial account number;
- student education records;
- intellectual property, such as certain intellectual property as set forth in
- Texas Education Code Section 51.914; or,
- medical records.

Custodian of an Information Resource: A person responsible for implementing owner-defined controls and access to an information resource. Custodians may include University employees,

vendors, and any third party acting as an agent of or otherwise on behalf of the University and/or the owner.

Information Resources: The procedures, computer equipment, computing facilities, software and data which is purchased, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

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.

Owner of an Information Resource: A person responsible for a business function and for determining controls and access to information resources supporting that business function.

Platform: A collective term for computer hardware and software components of a particular system. A platform includes a hardware architecture and a software framework (including application frameworks), where the combination allows software, particularly application software, to run. Typical platforms include a computer architecture, operating system, programming languages and related user interface (run-time system libraries or graphical user interface). Examples of common platforms would include servers, desktop/workstations, laptops, tablets, and smart phones. Special-purpose platforms include routers, remote access servers and database servers.

Security Patch: A change to a program that eliminates a vulnerability exploited by malicious hackers.

Server: A computer or program that supplies data or resources to other machines on a network.

Procedures and Responsibilities

1. PLATFORMS – SERVERS

1.1 Custodians of information resources shall ensure that vendor supplied patches are routinely acquired, systematically tested prior to implementation where practical, and installed promptly based on risk management decisions. Custodians are encouraged to have hardware resources available for testing security patches in the case of special applications.

1.2 Custodians of information resources shall remove unnecessary software, system services, and drivers.

1.3 Custodians of information resources 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 Procedure 29.01.03.H0.25 Malicious Code).

1.4 Audit logging shall also be enabled.

1.5 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.

1.6 Custodians of information resources shall disable or change the password of default accounts before placing the resource on the network. All passwords shall be enabled in accordance with Procedure 29.01.03.H0.11 Identification and Authentication

1.7 Servers shall be tested by custodians of information resources or their designee for known vulnerabilities, including application vulnerabilities, periodically or when new vulnerabilities are announced.

1.8 Custodians of information resources shall seek and implement recommended practices (such as security checklists) for securing the particular system platform(s) under their control.

2. PLATFORMS - OTHER THAN SERVERS

There are many varieties of platform types other than typical servers. Each type or device may have its own particular baseline security configuration and maintenance protocols. Owners or custodians of a platform should seek recommended practices (such as security checklists) for securing a particular platform. Security measures are to be implemented in a manner that will meet the requirements for confidentiality, integrity, and availability of the information being processed or stored.

3. EXCLUSIONS

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this procedure are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this procedure.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

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

Information Security Officer
903-886-5425