

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.21 Server Hardening

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Servers are relied upon to store and 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 increases manageability or prevents unauthorized access, unauthorized use, and disruptions in service.

The purpose of the university's server hardening procedures is to describe the requirements for installing a new server in a secure fashion and maintaining the integrity of the server, its application software, and the data it controls and maintains.

2. APPLICABILITY

This university procedure applies to all university information resources that store or process Sensitive Information.

The purpose of the implementation of this university procedure 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 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 university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources).

The intended audience includes, but is not limited to, computing system managers and administrators who manage university information resources that store or process Sensitive Information or systems that are deemed mission critical by their functionality.

3. DEFINITIONS

Please refer to University Procedure 21.01.06.C2.01 Definitions.

4. PROCEDURES

4.1. Information resources shall adhere to all university procedures before connection to the University network is permitted. Any information resource not in

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

compliance with university procedures may be removed from the university network until it is in compliance.

- 4.2. Resource custodians shall ensure that vendor supplied patches are routinely acquired, systematically tested when possible, and installed promptly based on risk management decisions.
- 4.3. To reduce exposure to vulnerabilities, resource custodians shall remove unnecessary software, system services, and drivers.
- 4.4. Resource custodians shall disable or change the password of default accounts. Other default configuration settings should also be changed based on risk management decisions for the information resource.
- 4.5. Resource custodians shall perform initial and periodic security testing of assigned information resources for known system and application vulnerabilities. This testing shall be done in accordance with University Procedure 21.01.06.C2.20 Security Monitoring and Scanning.
- 4.6. System and server hardening guidelines outlining minimum acceptable security configuration and implementation requirements for university resources shall be developed and published by Media and Computer Services. These guidelines shall serve as the base document for departmental guidelines relating to system and server hardening standards.
- 4.7. To maintain an operational and secure environment, resource custodians and department managers shall conduct a yearly risk assessment of system, network, and application deployment and configuration as per University Rule 21.01.06.C1 Network Security Information Resources.
- 4.8. Based on risk management decisions relating to an information resource's business function, resource custodians shall consider deploying additional security related software (e.g. firewalls, file integrity monitoring) not supplied by the resource's operating system or application vendor. The Information Resources Manager may require such protections for any university information resource.

5. CONSEQUENCES FOR VIOLATIONS

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
 - 01.03 Appointing Power and Terms and Conditions of Employment
 - 07.01 Ethics Policy, TAMUS Employees
 - 32.02 Discipline and Dismissal of Employees
 - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
 - 33 Employment, Standards of Conduct
- Texas A&M University-Corpus Christi Rule
 - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
 - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration