UNIVERSITY OF TEXAS ARLINGTON

Policy IT-PO1

Server Management Policy

Contents

I. Title
II. Policy
III. Definitions
IV. Relevant Federal and State Statutes and Rules
V. Relevant UT System Policies, Procedures and Forms
VI. Who Should Know
VII. UT Arlington Office(s) Responsible for Policy
VIII. Dates Approved or Amended
IX. Contact Information

I. Title

Server Management Policy

II. Policy

This policy establishes the requirements and the procedures for locating, installing, configuring, maintaining, patching, and monitoring the integrity of servers in a secure fashion at The University of Texas at Arlington ("University").

A. Responsibilities

General responsibilities regarding University server management are outlined below:

1. **Application Owner:** The application owner is responsible for:

    a. Ensuring compliance with all applicable policies and procedures in relationship to the server and application. Policies and procedures that are generally applicable to the administration of this policy are noted in the relevant rules, policies, and procedures sections of this policy.

    b. Ensuring a qualified application administrator is identified.

    c. Understanding what data will be managed by the application, the data's classification, and the appropriate data owner.

2. Ensuring the data is secured in accordance with the assigned data classification standard.

In addition, in the event an exception is granted for the location of the server, the application owner is also responsible
a. Ensuring a qualified server administrator is identified

3. **Application Administrator:** The application administrator is responsible for managing all aspects of the application and the reviewing of all appropriate logs.

4. **Server Administrator:** The server administrator is responsible for managing the hardware, networking, operating system, physical and other security of server(s), and the reviewing of all appropriate logs per the UT System Information Resources Use and Security Policy ("UTS165").

Application and server administrators are responsible for ensuring the application owner is informed in a timely matter of any issue in relationship to the server and/or application.

B. Purchase

An application owner must obtain the Vice President of Information Technology's approval of a server hardware request before proceeding to acquire such server hardware. In obtaining such approval, the application owner must demonstrate to the Vice President of Information Technology the business need for the server hardware. All server hardware must be acquired and provisioned by the Office of Information Technology unless an exception for the purchase and provisioning has been approved by the Vice President of Information Technology.

C. Location

All servers must be located in a location that is approved by the Office of Information Technology.

D. Network Configuration

All servers, when applicable, will:

1. Be registered to the UTA domain
2. Utilize approved static IP address(es)
3. Utilize approved network protocol(s)
4. Utilize wired network connectivity
5. Disable all unnecessary operating system and application services

E. Authentication

All access must utilize an approved University enterprise authentication method. All accounts must be managed in accordance with all applicable account management policies and procedures noted in the relevant rules, policies, and procedures sections of this policy.

F. Password Protection

All accounts must comply, when applicable, with UT System Identity Management Federation Member Operating Practices.

G. Remote Administration

All administrative access to a server from off campus must utilize the University's Virtual Private Network ("VPN"). Information on accessing the VPN can be found at www.uta.edu/vpn.

H. Logs

All applicable logs generated by the application must be secured and retained in accordance with University's Record Retention and Information Management Schedules. All other logs must be secured and retained in accordance with applicable log retention requirements. Administrators will regularly review all applicable logs.

I. Backups

All application owners should ensure there is a documented backup plan for the restoration data in accordance with the UTS165.

J. Security Updates

The latest patches for all applicable operating system and application software will be applied in a timely matter by the respective administrators. All patches should be tested prior to being installed when practical.

K. Server Hardening Standards

All servers will be security hardened based on risk analysis and must comply with the University's server security configuration baseline approved by the University's Information Security Officer.

L. Firewall

All servers must be protected from unauthorized access and all network access to all servers will be configured to deny all non-essential traffic unless an exception is granted by the Information Security Officer.

M. Malware Protection

All servers are required to have installed an anti-malware application. Use of the University's approved centrally managed clients, when available, is required. Use of any other anti-malware application must be approved in advance by the Information Security Officer. Server administrators will ensure the regular scanning of all servers and ensure the remediation of any findings.

N. **Sensitive Information**

All administrators will ensure that data stored on the server is scanned using a scanning application that is approved by the Information Security Officer at least once every six months. If vulnerabilities are discovered during those scans, remediation must be initiated and the Information Security Office must be notified immediately.

O. **Vulnerability Assessment**

A server may not be used in a production capacity until it is secured and has been approved by the Information Security Office. The Information Security Office reserves the right to scan a server at any time and to initiate remediation procedures if vulnerabilities are discovered.

P. **Removal of Data**

All data associated with the server must be removed prior to the sale or transfer of the equipment in accordance with Texas Administrative Code ¤202.78.

Q. **Exceptions**

Any server that cannot comply with this policy may be granted an exception after a review and approval by the Information Security Officer and by the Vice President of Information Technology. If a department requesting an exception to this policy on the basis of non-security-related issues disagrees with the decision of the Information Security Officer and the Vice President of Information Technology, the department may appeal the decision to the Vice President for Academic Affairs, who has final approval authority for the exception. However, under UTS 165, the Vice President for Academic Affairs may not grant an exception to this policy if the Information Security Officer has determined that security of the server is at risk.

R. **Consequences**

If the Information Security Officer or the Vice President of Information Technology determines that the application owner, who has obtained an exception under the provision of this policy, is unable to maintain appropriate server administration, the Office of Information Technology will take control of the server for ongoing maintenance with provisions made for the appropriate academic/administrative use. An individual's violation of this policy may result in disciplinary action which may include the termination of the individual's access to any or all University information resources as well as (1) termination or suspension of employment, if the individual is a University employee; (2) termination or suspension of any contract or other relationship with the individual, if the individual is a contractor, consultant, or temporary worker; (3) dismissal if the individual is an intern or volunteer; or (4) suspension or expulsion if the individual is a student.

S. **Special Instructions for Initial Implementation**

1. Servers not located in an approved location must be relocated to an approved location within 18 months of the approval of this policy.

2. The Office of Information Technology may choose to transfer the function of a relocated server to other hardware if the Office of Information Technology determines that doing so would minimize the costs to the University and provide functionality that is equivalent to the server from which the function is transferred.

III. Definitions

Access: The physical or logical capability to interact with, or otherwise make use of information resources.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system failure.

Change: Any addition, modification or update, or removal of an Information Resource that can potentially impact the operation, stability, or reliability of a University network or computing environment.

Control: A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Custodian: An individual or entity responsible for implementing Owner-defined controls and access to an Information Resource. Custodians include Information Security Administrators, University information technology/systems departments, vendors, and any third party acting as an agent of or otherwise on behalf of the University.

Custodian of an Information Resource: A person responsible for implementing the information owner-defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the University.

Data: Recorded data, regardless of form or media in which it may be recorded, which constitute the original data necessary to support the business of the University or original observations and methods of a study and the analyses of such original data that are necessary to support Research activities and validate Research findings. Data may include but is not limited to: printed records, observations and notes; electronic data; video and audio records, photographs and negatives, etc.

Decentralized Areas: University business units, departments, or programs outside of the Office of Information Technology that manage or support their own information systems.

Digital Data: The subset of Data (as defined above) that is transmitted by or maintained made available in, electronic media.

Encryption: The conversion of plaintext information into a code or cipher text using a variable, called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

Firewall: A software or hardware device or system that filters communications between networks that have different security domains based on a defined set of rules. A firewall may be configured to deny, permit, encrypt, decrypt, or serve as an intermediary (proxy) for network traffic.

Information: Data organized, formatted and presented in a way that facilitates decision making. All information is data.

Information Resources: Any and all computer printouts, online display devices, mass 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 data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDAs), 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.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, information, data, applications, communications and people.

Integrity: The accuracy and completeness of information and assets and the authenticity of transactions.

Owner: The manager or agent responsible for the business function that is supported by the information resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security and authorizing access to the information resource. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared.

Password: A string of characters used to verify or "authenticate" a person's identity.

Research: Systematic investigation designed to develop and contribute to knowledge and may include all stages of development, testing and evaluation.

Security Incident: An event which results in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.

Sensitive Data: Digital Data that requires higher than normal security measures to protect it from unauthorized access, modification or deletion. Sensitive Data may be either public or confidential and is defined by the University based on compliance with applicable federal or state law or on the demonstrated need to (a) document the integrity of that Digital Data (i.e., that the Data had not been altered by either intent or accident), (b) restrict and document individuals with access to that Digital Data, and (c) ensure appropriate backup and retention of that Digital Data. These would most frequently be required by:

- Federal agencies (e.g., Food and Drug Administration);
- State agencies (e.g., data defined as High-Risk Information Resources by 1 TAC 202.72);
- Employee benefit providers;
- Office of General Counsel or University's Office of Legal Affairs (i.e. data subject to or involved in litigation or confidentiality agreements);
- Intellectual Property and /or Technology Transfer requirements; or
- Federal regulations (e.g., FERPA, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, Biodefense, Homeland Security, DOD etc.)

Server: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Vendor: Someone outside of the University who exchanges goods or services for money or other consideration.

IV. Relevant Federal and State Statutes and Rules

Texas Government Code, Chapter 2054, "Information Resources"

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C; Security Standards for Institutions of Higher Education

V. Relevant UT System Policies, Procedures and Forms

UT System Administration Policy UTS165; UT System Information Resources Use and Security Policy

University of Texas at Arlington Data Classification Standard

VI. Who Should Know

All individuals authorized and responsible for the installation and management of any University information resource; including all information resource data and application owners, and server and application administrators.

VII. UT Arlington Office(s) Responsible for Policy

Information Security Office

Office of Information Technology

VIII. Dates Approved or Amended

Approved: 01/16/2018

IX. Contact Information

Information Security Officer
security@uta.edu
(817) 272-5487

Vice President of Information Technology
cio@uta.edu
(817) 272-0202

A. Title

Write your text here!

B. Title

Write your text here!