SERVER MANAGEMENT AND STANDARDS
07.200.02

Authority:	CIO
History:	Updated May 25, 2021; reformatted June 6, 2005; supersedes policy ITS 2.00; effective September 11, 2002
Source of Authority:	UNC System Office Policy Manual, Chapter 1400 "Information Technology" International Organization for Standardization ISO/IEC 27002
Responsible Office:	Information Technology Services

I. Purpose

This document provides policies and guidelines for the responsible management and administration of the University of North Carolina Wilmington's enterprise servers.

Also see UNCW Policy 07.200.09 "Distributed Information Technology Management."

This is not a comprehensive document covering all aspects of responsible management. The following are intended to establish a framework of principles, guidelines and operational procedures that ensure the effective, efficient, secure management of the enterprise servers consistent with the mission and goals of the university.

Information Technology Services (ITS) has the responsibility for the effective, efficient, and secure management of enterprise servers that provide enterprise, mission critical services to the university community such as ERP, e-mail, Web, collaboration, and a number of Web-based and Web-enabled applications supporting a host of academic and administrative services. ITS administers baseline standards that centralized servers must follow concerning compatibility, security, interoperability, and data integrity.

II. Policy

Campus enterprise servers are mission critical resources that may be utilized by all members of the campus community. It is essential, therefore, that these resources be managed effectively to ensure maximum availability, accessibility, security, and operational efficiency in support of academic offerings and administrative requirements.

A. Enterprise Server Operating System Software (ESOSS)

a. ESOSS supported by ITS are based on university needs and ability to be supported.
b. The level of operating system support provided by ITS for non-enterprise servers vary based on the applications running on the server and the availability of support personnel.

However, all systems must be kept current with patches, security, and managed with best practices.

c. ITS is responsible for determining the need and relevancy of ESOSS updates, service releases, and emergency patches. ITS staff will take appropriate action depending on the urgency of the update.
d. ITS will endeavor to inform all affected individuals of ESOSS changes and possible issues which might arise from those changes in a timely manner. ITS staff will attempt to minimize the negative impact on users through flexibility in scheduling and university preapproved scheduled maintenance windows.
e. All ESOSS updates on production systems will be implemented in accordance with the Change Control Procedure.
f. ITS will maintain access to all current ESOSS.

B. Application Software

a. All software to be installed on the university's enterprise systems must be approved by ITS.
b. Application owners must inform ITS staff of any significant changes in software.
c. All application changes will be implemented in accordance with the Change Control Procedure. Emergency updates, as determined by ITS, will be given priority over previously scheduled events.
d. Applications may be disabled or removed from university systems at the discretion of ITS for specific reasons. Reasons would include, but not be limited to:
    i. Poses a credible security risk.
    ii. Malfunctions or functions in an unauthorized manner.
    iii. Causes the operating system to be unstable.
    iv. Causes other applications to malfunction.
    v. Causes or has strong potential of causing data loss.
    vi. Is not supported for the current version of the operating system.
e. Application owners are ultimately responsible for the accuracy and validity of application data.
f. Application owners are responsible for informing their constituent user population of changes or updates.
g. Application software must be maintained to be compatible with the current operating system version.
h. All applications, regardless of cost, installed on enterprise systems must be vetted by ITS prior to acquisition.

C. Hardware

a. ITS will endeavor to implement "state of the art" computer equipment to support the campus mission and to ensure that all equipment meets university requirements for stability, reliability, and security.
b. Support for applications and software that aligns with the university mission will be the determining factor in the decision to support a new hardware platform or remove an existing platform.

c. ITS will strive to minimize the number of hardware platforms to the minimum required to accomplish the University's mission.
d. Depending on the nature of the supported applications, ITS may require external (vendor or contracted) support for hardware and operating system environments.

D. Disaster Recovery

a. ITS is responsible for maintaining, testing, and continuously improving the plan for recovery of enterprise servers in the event of a disaster. Details can be found in the ITS Disaster Recovery Manual.
b. ITS will take all reasonable measures to ensure the safety, security and recoverability of data stored on supported systems.
c. The order of restoration of services is dependent upon the scope and extent of the disaster and the number of failed systems.
d. When possible, ITS will maintain a secondary computing site with computer hardware available to rapidly allow some level of restoration of service.
e. Cloud based solutions should be considered for critical systems for disaster resilience.

E. Departmental Servers

Also see UNCW Policy 07.200.09 "Distributed Information Technology Management."

a. Departmental servers are not recommended. The avoidance of duplication of effort is a priority to conserve financial and human resources.
b. All servers owned by UNCW or residing on the UNCW network must conform to UNCW policies.
c. ITS and decentralized system administrators must take all reasonable care to enable only services on a server that are required to fulfill the function of that server.

F. Networking

a. ITS will only utilize network protocols defined in Policy 07.200.03 "Network Infrastructure Management and Standards."

G. Mobile Devices

a. Mobile Devices that require access to servers must adhere to the same standards as desktop and laptop computers. Users must implement appropriate security precautions on the mobile device and authenticate with a username and password before access is allowed.