I. Purpose

This document provides policies and guidelines for the responsible management and administration of the University of North Carolina Wilmington’s servers and multiuser computers.

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

The Information Technology Systems Division is charged by the Chancellor of the university with responsibility for the effective and efficient management of servers and multiuser computers that provide enterprise, mission critical services to the university community such as ERP, e-mail, Web, file and printer sharing, and a number of Web-based and Web-enabled applications supporting a host of academic and administrative services. The Department of Operations and Systems Administration (OSA) within the Information Technology Systems Division is charged by the Chancellor to establish and administer baseline standards that decentralized servers and multiuser computers must follow concerning compatibility, security, interoperability, and data integrity.

II. Policy

Campus servers and multiuser computers are mission critical resources that are utilized by all members of the campus community. It is essential, therefore, that these resources be managed effectively to ensure maximum availability, accessibility, and operational efficiency in support of academic offerings and administrative requirements. OSA works to ensure that the allocation of resources meets the needs of the faculty, staff, and students and aligns with university goals and standards and are utilized in the most effective manner possible.
A. Administrative Provisions

1. Operating System Software

   a. Operating systems supported by OSA are based on university needs and, in many instances, determined by the application vendor.
   b. The level of operating system support provided by OSA for decentralized servers varies based on the applications running on the server and the availability of support personnel.
   c. OSA is responsible for determining the need and relevancy of operating system updates, service releases, and emergency patches. OSA staff will take appropriate action depending on the urgency of the update.
   d. OSA will endeavor to inform all affected individuals of operating system changes and possible issues which might arise from those changes well in advance. OSA staff will attempt to minimize the negative impact on users through flexibility in scheduling updates.
   e. OSA will take all reasonable steps to ensure data integrity during system updates.
   f. All operating system updates on production systems will be implemented in accordance with the Change Control Procedure.
   g. OSA will maintain a current system software inventory.

2. Application Software

   a. All software to be installed on the university’s production systems that are managed by OSA must be approved by the Director of OSA.
   b. Application owners must inform OSA 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 the director, will be given priority over previously scheduled events.
   d. Applications may be disabled or removed from university systems at the discretion of OSA and IT Security for specific reasons. Reasons would include, but not be limited to:
      i. Malfunctions or functions in an unauthorized manner.
      ii. Causes the operating system to be unstable.
      iii. Causes other applications to malfunction.
      iv. Causes or has strong potential of causing data loss.
      v. Poses a credible security risk.
      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. Applications software must be maintained to be compatible with the current operating system version.

3. Hardware
a. OSA will endeavor to implement “state of the art” computer equipment to support the
campus mission. The department will work 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. OSA will strive to minimize the number of hardware platforms to the minimum
required in order to accomplish the University’s mission.
d. Depending on the critical nature of the supported applications, OSA may require
external (vendor or contracted) support for hardware and operating system
environments.
e. OSA will maintain a current hardware inventory.

4. Disaster Recovery

a. OSA is responsible for maintaining, testing and continuously improving the plan for
recovery of servers and multiuser computers in the event of a disaster. Details can be
found in the ITSD Disaster Recovery Manual.
b. OSA 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 dependant upon the scope and extent of the
disaster, the number of failed systems, and the level of importance to the university of
a system as defined in the ITSD Disaster Recovery Manual.
d. When possible, OSA will maintain a secondary computing site with computer
hardware available to rapidly allow some level of restoration of service for the
highest priority systems as defined in the ITSD Disaster Recovery Manual.

5. Departmental Servers

a. Departmental servers are not recommended without proper support personnel within
the department and without prior consultation with OSA. The avoidance of
duplication of effort is a priority to conserve financial and human resources.
b. Servers administered and maintained by departments will not be supported by OSA
staff unless they are in compliance with UNCW Server Protocols. All servers owned
by UNCW or residing on the UNCW network must conform to the UNCW Server
Protocols and must have a disaster recovery plan referenced by the ITSD Disaster
Recovery Plan.

6. Networking

a. OSA will only utilize network protocols defined under Network Standards and
Management.
b. OSA 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. For
example, if Web services are not needed on a server then port 80 should not be open
on that server.

7. Streaming Video Services
a. Media files are to be served from the campus supported media content server(s) or iTunes U.

8. Handheld and Pocket PC’s

   a. Handheld and Pocket PC’s that require access to servers and multiuser computers must adhere to the same standards as desktop and laptop computers. Users must authenticate with a username and password before access is allowed.

9. Security and Encryption

   a. All password information must be stored in encrypted format on all electronic resources.

   b. Encryption standards are recommended by OSA staff to the Director of Operations and Systems Administration and approved by the Vice Chancellor of the Information Technology Systems Division.