Subject: Message from Chancellor Martin re: Information Technology Infrastructure
Importance: High

To: Deans, Directors, and Department Heads

From: Michael Martin, Chancellor

Addendum to July 2007 Memorandum on Leadership, Responsibility, and Authority for the Security of LSU's Information Technology Infrastructure

In memorandums dated July 17, 2007 and February 20, 2008 from the Office of the Chancellor, the importance of securing and maintaining the information technology resources of the University was stressed. In addition, the memorandum confirmed Brian Voss, the Vice Chancellor for IT and CIO (VCIT) as being charged with ensuring the security of information technology at LSU and compliance with LSU System PM-36, the Louisiana State University System Information Security Plan. PM-36 requires that LSU follow best practices as embodied in the ISO/IEC 27002 standard. These standards provide a roadmap for the appropriate management and securing of information technology resources at LSU. Ensuring that proper backups are maintained, that important and sensitive data is protected, and that plans for the continuity of services are documented are essential parts of these standards and are thus, required for the campus to be in compliance with PM-36.

LSU System Internal Auditing recently performed a follow-up review of its **2007 audit** of the LSU campus regarding compliance with PM-36, and issued a report of findings, including recommendations regarding the use of distributed servers for electronic mail (e-mail) and other purposes outside of centrally managed systems. To promptly address these audit findings and recommendations, I am directing that the following actions be taken immediately relative to the operation of e-mail and other servers operating in the colleges, departments, and affiliated organizations.

1. All Deans, Directors, and Department Heads shall submit a letter of justification and request for approval describing each server employed within their colleges and departments to the **VCIT** by **April 30, 2010**. Specifically, these letters must address reasons for the need to operate each separate e-mail or other server outside of the central IT enterprise.

2. Upon approval from the VCIT for any distributed e-mail or application server to remain in operation in departments, an acceptable disaster recovery and business continuity plan shall be submitted to the **LSU Emergency Operations Center** no later than **May 1, 2010**.

   For E-mail or other servers not approved by the Office of VCIT, plans shall be made to remove them from service and their functions migrated to centrally-offered or managed environments no later than **June 30, 2010**.

3. On **July 1, 2010**, e-mail and other servers in operation that have not completed the above requirements shall be disconnected from the LSU campus network.

   The above procedures are required of all colleges, departments, and affiliated organizations operating e-mail or application services on the LSU network.

   You will be contacted by representatives from the VCIT shortly with details regarding any servers of which ITS is aware that exist within your departments. You are urged to have your local IT staff prepare an inventory of servers as well, to compare with the report from ITS. Please contact ciso@lsu.edu or call 8-3724 if you have any questions in the meantime.

   cc: Vice Chancellors
           Vice Provosts
           D'Ann Morris, Interim Director of Emergency Operations
           Brian Nichols, Executive Director for Risk Management