LOUISIANA STATE UNIVERSITY

CAMPUS CORRESPONDENCE

To: Deans, Directors and Department Heads **Date:** February 26, 2008

From: William L. Jenkins
President Emeritus and Acting Chancellor

College and Departmental Disaster Recovery/Business Continuity Plans (DR/BCP)

Over the years, dependence upon the use of information technology (IT) in the day-to-day business operations of many organizations has become the norm. Louisiana State University certainly is no exception to this trend. Today we find very powerful computers in many colleges and departments on campus. These machines are linked together by a sophisticated network that provides communication with other machines across campus and around the world. Vital functions of the University depend on the availability of this network of computers.

Many colleges and departments offer services outside of LSU centralized computing such as e-mail, file storage, and specialized applications. These functions, which are often critical to the unit's ability to conduct day-to-day operations, are not included in the centralized DR/BCP. Inadequate DR/BCP implementation and testing increases the risk for loss of critical IT functions, as well as loss of business, instructional, and research data in the event of a disaster. This was, in fact, highlighted in a recent LSU System audit of the LSU campus for compliance with PM-36.

In response to that audit's finding and in order to reduce the risk for loss of essential IT functions, I am directing that all critical IT services and applications be centrally managed where feasible. However, all colleges and departments that have a legitimate business need to operate their own services must develop, document, and test their DR/BCP on an annual basis. A copy of these college- or department -pecific DR/BCP documents, any amendments, and results of testing must be submitted to the Emergency Operations Center (EOC) annually for review and to be kept on file.

cc: Vice Chancellors, Vice Provosts