TO: University Faculty and Staff

FROM: Modesto A. Maidique, President
       Ronald Berkman, Executive Vice President and Provost

DATE: July 2, 2007

SUBJECT: Information Technology Security at FIU

Our FIU information technology resources hold a great amount of sensitive information about our students, employees, alumni, donors and soon to be patients. Federal and state laws require that the University implement and maintain standards that ensure this information is protected from unauthorized access and use. As part of our effort to secure our information resources and information systems, we are announcing that the Division of Information Technology has recently begun to roll out a critical information technology security initiative aimed at increasing the security of our desktop and laptop computers that use the Microsoft Windows® operating system. As you may recall, the two breaches of sensitive information that took place at FIU in 2005 and 2006 were the result of desktop computers being compromised.

The name of the technology, Active Directory, will provide greater security to the information maintained in the University's desktop and laptop computers. Just like cars, computers need regular maintenance and Active Directory provides a method to manage the tools that help UTS and campus Information Technology Administrators maintain the basic security for the computers you use on a daily basis. Active Directory is a system that will facilitate user authentication with central password management, operating system management, anti-virus patch management and sensitive data encryption.

In order for the University to be successful in securing its computing environment, all employees who work with a university laptop or desktop computer that relies on the Windows operating system shall join either the UTS Active Directory Domain or become a member of their department's Active Directory which meets required minimum security standards. Wireless and remote users will have the same security measures that are being implemented through Active Directory applied to their off-campus computers or their wireless computers via network access controls. In addition, the IT Security Office will work closely with those individuals who rely on operating systems other than Windows, or who maintain data subject to specific security restrictions (usually in the case of research data), in order to ensure that their computers meet minimum security standards that will not expose the University to data loss or compromise.

The implementation of Active Directory has already begun in several administrative units. Your departments will be receiving additional information regarding the Active Directory implementation directly from our CIO, Dr. Min Yao. In addition, you may view other details regarding this implementation including time line, frequently asked questions, etc. by visiting http://fiuad.fiu.edu.