EFFECTIVE DATE: **Revised November 2008**

SUBJECT: **Security of Information Technology Systems and Networks**

AUTHORIZATION: _____

Christopher J. Rogers, Director of Technology Services

I. **POLICY:** Southern University Agricultural Research and Extension Center (Southern University Ag Center) employees shall follow defined security practices in use of information technology systems and networks to protect the Southern University Ag Center, its faculty, staff, administrators and resources. Information Technology Systems and Networks includes, but is not limited to, hardware, software, communications networks, physical facilities, mainframe computer, personal computers and printers, and personal hand held devices.

II. **PURPOSE:** To protect information technology systems and networks within the Southern University Ag Center.

III. **APPLICABILITY:** Applies to all employees within the Southern University Ag Center.

IV. **PROCEDURE:**

PASSWORDS
The proper use of a secured, confidential password is the easiest and most effective security tool available. Passwords should not be divulged to other persons and must be changed on a regular basis. The Office of Technology Services (OTS) has integrated its policy with the State of Louisiana – Office of Computing Services state standards for passwords in IT STD-009. The Office of Computing Services (OCS) guidelines for LAN passwords are documented in:

http://www.doa.state.la.us/ocs/security/password.htm

Southern University Ag Center shall periodically audit password use within the State of Louisiana – Office of Computing Services for compliance to established standards.

VIRUSES

All computers connected to the Southern University Ag Center's LAN including employee/non employee desktops and laptops must have current anti-virus software installed and enabled. The virus definition updates and scans shall be scheduled to occur at least once a week.

WIRELESS DEVICES

Wireless networks have been proven to present security problems and require additional layers of protection to prevent unauthorized access. No wireless computer network system may be established or accessed within Southern University Ag Center, A. O. Williams Hall except those specifically authorized by the Office of Technology Services (OTS).

LOCKDOWN

OIT Policy No. 005 defines the benefits and statewide guidelines for desktop power management and lockdown. To maximize security, facilitate support, and reduce costs, the OTS will disable administrative privileges on standard desktops. Based on business needs, a OTS section may request an exception be made for desktop power management and lockdown.

The power management features shall be enabled on all desktop computers. Employees are expected to power off desktop computers and peripherals at the end of each work week.

SERVERS

No computer will be configured as any kind of server on the Office of Technology Services (OTS) networks without written approval from the OTS Director. Servers that will be accessed from more than one location must be housed within a Southern University Ag Center's server farm environment.

V.   RESPONSIBILITIES:

<u>EMPLOYEE</u>

The employee is responsible for adhering to the published IT security policies and take reasonable steps to protect Southern University and the State of Louisiana computer systems and networks. If a virus is transmitted to a user's personal computer, the user is responsible for immediately informing the Office of Technology Services. Each employee is also

responsible for powering off desktop computers and peripherals at the end of each work week.

OFFICE OF TECHNOLOGY SERVICES

Office of Technology Services (OTS) is responsible for the management and control of networks within the Southern University Ag Center. OTS will establish standards for wireless network use.

The OTS Director is responsible for the review and approval of requested exceptions to the lockdown policy to ensure PC configuration changes associated with requested software will not interfere or jeopardize network security.   OTS shall document and update the specific guidelines for password usage, incorporating IT standards and industry practices. OTS shall check passwords periodically for adherence to rules, where possible. The OTS Director is responsible for approving any servers within the Southern University Ag Center.