# Financial Systems Services Computer Support Policy

**Scope:** This policy applies to all hardware, data, and software which fall under the support of FSS.

**Overview:** This document will outline Financial Systems Services' (FSS) approved guidelines and procedures for units which are supported by the FSS staff. This document should be used in conjunction with the official LSU acceptable use policy (http://itsweb.lsu.edu/ITS_Security/IT_Policies/LSU/item614.html). It is the responsibility of every user to know these guidelines and to conduct his or her activities accordingly.

## 1) Support Guidelines

*The FSS support role will include the following:*

a) FSS will make all computer-related hardware purchases
b) FSS will support all computing devices that are considered LSU property
c) FSS will have a 5 year lifecycle replacement of computer hardware (PC Only)
d) FSS will pre-configure all hardware prior to delivery to user
e) FSS will install and maintain the University-approved and managed antivirus software
f) FSS will respond to any hardware/software issues that cannot be resolved at a user level
g) FSS will be responsible for group policy/active directory management
h) FSS will provide file/print sharing through FSS servers
i) FSS will provide security access to data systems under the support of FSS

*The FSS Support role will **not** include the following:*

a) Personal Data stored on FSS/LSU supported equipment
b) Non work-related software
c) Assistance with personal computing devices

## 2) Audit Policy

a) Purpose
    i) Ensure integrity, confidentiality and availability of information and resources
    ii) Investigate possible security incidents to ensure conformance to LSU security policies
    iii) Monitor hardware/software changes
    iv) Monitor documents which may contain sensitive personnel information (SSN, Credit Cards)
b) Policy
    i) All FSS network staff will have administrative access to each machine
    ii) This access may include:
        (1) User level and/or system level access to any computing device

(2) Access to any electronic information that may be produced, transmitted or stored on FSS supported equipment
(3) Access to work areas

iii) This access will not include:
(1) Personal Data
(2) Email

c) Hardware/Software audits are done remotely when a computer is powered on/restarted.

d) FSS receives a security audit report monthly from ITS that details any security flaws/unpatched software found. If found, FSS will apply any applicable patches/fixes.

**3) Data Backup Procedure**

a) All work-related information stored on FSS servers are backed up nightly using an incremental backup system.

i) FSS will create and install applicable network shares for FSS supported devices. Users are responsible for saving critical data to FSS servers using the departmental shares created and installed by FSS.

ii) Personal directories (i.e. – HOME directories) are not considered mission critical and no mission critical data should be stored on them. These folders will not be considered high priority in the event of a data loss.

iii) In the event that a server fails, any files created/modified since previous backup will not be available.

iv) Recovery timeframe will be determined by the extent of data loss and size of data files.

b) All files located on any local user machines are not backed up by FSS.

**4) Sanitation Policy**

The purpose of this policy is to protect the intellectual property of LSU and the confidentiality of its employees, etc. It defines the data sanitization standards and procedures to be used in the pre-disposal of hardware.

a) Method

i) Equipment will be sanitized using an approved DOD method or degaussing where applicable.

ii) If equipment is unable to be sanitized using this method, FSS will restore device to factory condition prior to surplus.

**5) Security Access for Users**

FSS will utilize a policy of "lowest level privileges adequate for the task." This helps to reduce threats to network and data security, and if a system is compromised it can be contained to a smaller area of the network/data and not invade larger areas. This shall apply to any databases, equipment, and applications systems that are supported by FSS.