SOUTHWEST TENNESSEE COMMUNITY COLLEGE

SUBJECT: **Mobile Computing Device Policy (**Formerly**: Laptop Policy)**

EFFECTIVE DATE: February 4, 2002 / Rev: January 21, 2010 ;Rev : January 21, 2015

The Mobile Computing Device Policy will be consistent with and not supersede other Southwest Tennessee Community College policies, including the Information Systems "Acceptable Usage Policy."

A. General

The term "mobile computing device" refers to a portable computing or telecommunications device that can execute programs. This definition includes, but is not limited to: laptops, tablets, PDAs, smart phones, and cell phones. **For information regarding mobile devices other than laptops please refer to Southwest Tennessee Community College's Mobile Communication Policy No. 4:03:04:00/22.**

Mobile computing devices will be ordinarily deployed in three different ways at Southwest Tennessee Community College:

1. As a resource assigned to an individual to replace the standard desktop PC, usually when a faculty or staff person is required to work regularly at more than one location.

2. As a resource intended for shared use within a department to support a certain function within the department.

3. As a resource assigned to a central agent within the College (e.g., the Library) that will make the equipment available for loan to any faculty or staff on a short-term basis.

4. A faculty member or staff who is required to regularly work at more than one location.

Source of Policy:	**Information Technology**	**Responsible Administrator:**	**Executive Director of Information Tech. Services**
		TBR Policy Reference:	**N/A**
Related Policy:	**N/A**	**TBR Guideline Reference:**	**N/A**
Approved:	 **President**	**Date:**	**June 1, 2015**

B. Deployment Guidelines

1. In order to acquire a mobile computing device, the requestor must first complete a standard form (Attachment A) which will document such information as the requestor's name, department, source of funding, desired applications, rationale for the acquisition, etc. The form requires approval from the requestor's department, Dean or Executive Director, and Information Technology Services. This form will accompany a fully approved Purchase Requisition.

2. The Information Technology Services department will be responsible for the specification, acquisition, and support of the mobile computing device.

3. The individual in possession of a mobile computing device must execute a personal responsibility form (Attachment B) affirming that he or she is familiar with the basic guidelines for securing the equipment, and that he or she also understands the obligations of laptop computer use.

C. Mobile Computing Devices Ownership and Use Issues

1. If the laptop is to replace a standard desktop microcomputer, then consideration should be given to furnishing the laptop with a docking station and attached accessories such as an external monitor, keyboard, mouse, network connection, etc.

.

2. Assuming that remote connection will be desired, consideration needs to be given to the type of remote Internet connection method, i.e. ISP or campus dial-up service.

3. Software loaded on a computer owned by the College is subject to the terms and conditions of pertinent software license agreements; all institutional software policy and guidelines must be followed.

4. Security and integrity of data files is the responsibility of the user. Consideration should be given to the location of data files (whether on a College server, the fixed drive in the computer, or an encrypted removable media). Back-up of data not stored on a College server is the sole responsibility of the end user.

5. All mobile and removable devices, such as, laptops, tablets, and removable media (USB drives, thumb drives, external drives, etc.) that contain or will contain student data should be encrypted with the college encryption software before storing data on the device.

6. **Refer to Acceptable Computer Usage Policy sections 1.3.2 and 1.3.3 and 1.3.4. and 2.4**

D. Mobile Computing Device Security Guidelines

All data files on the mobile computing devices and all data files on any removable media devices used in conjunction with the mobile computing device shall be encrypted and password protected for security purposes. All personally owned mobile devices that provide access to college privileged data such as e-mail, VPN, calendar events, etc., shall be protected by the lock codes provided by the devices operating system.

Use of the following guidelines will help minimize the theft risk of a College-issued mobile computing device.

1. Know where the laptop is at all times. Police and security officers unanimously agree that a laptop out of sight – even for a few seconds – is an easy mark.

2. Keep the laptop in a satchel, briefcase or other nondescript bag. Standard cases designed specifically for your laptop clearly portray their contents, making it an easier target for the thief to spot in a crowd. Cases containing the machine should also be locked with a simple luggage lock to provide some element of deterrence and delay.

3. Do not leave a laptop visible in an unattended motor vehicle. Lock the computer in the trunk.

4. The doors to labs and office spaces should be secured whenever your laptop is left unattended. If possible, the laptop should be stored in a locked file cabinet or secured with a locking device.

5. Identify the case in some unusual way to make it stand out from all other bags. An unusual color, special large tags or bright balls or flowers attached to the bag will give you a greater immediate ability to locate the bag and give police probable cause to stop and question the carrier.

6. Clearly identify the laptop with a visible nametag on the bag and by writing your name, address and telephone number on the case. Verify that the laptop has an institutional inventory tag firmly attached. Place your business card inside the bag and reprint your identifying information in the battery compartment and/or on the battery itself.

7. While commuting in a taxi, shuttle bus or public transportation, keep the laptop with you at all times. Do not permit the driver to load your laptop as baggage where it may be out of your view.

8. Keep the laptop as a carry-on. Placing your laptop in the baggage compartment easily exposes it to the rigors of the baggage handling process and risks theft by dishonest employees. Place the laptop in the under-seat storage area where you have more control if possible, rather than in an overhead bin.

All users of Southwest Tennessee Community College computer and telecommunications resources are expected to read and abide with the college’s Acceptable Computer Usage Policy.

Attachment A:

MOBILE COMPUTING DEVICE REQUEST

This Form is Intended to Aid in Assessing Mobile Computing Device Requirements

Date: _______________________ Campus/Location: _________________

Department: _________________ Contact: __________________________

Account Number: _____________ Contact Telephone: _________________

Type of Device being requested: (check one)

Laptop:_____ Tablet:_____ Printer:_____ Monitor:_____ Scanner:_____

Brand of Device:_____________________________ Size:______________________

Describe how Laptop will normally be used:
(List required application software)

List additional hardware required:

______ Monitor ______ Docking Station Other:_________________
______ Keyboard ______ Extra Batteries

Will the Laptop contain student data? (yes/no) **_______________________________**

Approximate number of hour per week unit will be utilized: ___________________

Will this request replace an existing device: (Yes/No) _________________________

Prepared By: ______________________________________ Date: ____________

Dept. Head/Director: ________________________________ Date: ____________

Additional Approval: ________________________________ Date: ____________

Info Sys Representative: _____________________________ Date: ____________

Attachment B:

Personal Responsibility Form

Name: ___________________________ Campus/Location: _________________

Department: ______________________

Equipment Description: ____

____

____

Equipment Serial Number: ____

Southwest Tennessee Community College Asset Tag Number: _________________

I have read and understand the Security Guidelines in the Laptop Computer Policy.

I understand that I may be personally liable for the loss of College equipment in my possession.

Will your laptop or tablet contain student data or other College privileged information?

□ **Yes** □ **No**

If you check no, it is your responsibility to contact the Information Technology Services department to encrypt your device if student data is going to be stored on your device.

Signed: ______________________________________ Date: ____________