SOUTHWEST TENNESSEE COMMUNITY COLLEGE

SUBJECT: Mobile Computing Devices

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

Revised July 1, 2024

*In October of each year, Information Technology related policies are reviewed as required by external regulations.

Purpose

The purpose of this policy is to set forth guidelines for the use of mobile computing devices that store the sensitive information of Southwest Tennessee Community College ("Southwest" or "the College"), whether the information is on a College-owned device or one not owned by the College, in an effort to protect the College's network and information from unauthorized access and disclosure.

Definition

Mobile Computing Device- portable computing or telecommunications equipment that can execute programs, including, but not limited to: laptops, tablets, personal digital assistants (PDAs), smartphones, cell phones, storage media such as USB hard drives, memory sticks, flash drives, thumb drives, secure digital or compact flash cards, CD-R or DVD-R media, and any peripherals connected to a mobile device. For information regarding mobile communication devices other than laptops, please refer to the College's Mobile Communication Policy, 6:03:04:00/22.

Policy

General

It is intended that this policy be consistent with and not supersede any other College policies, including the Acceptable Usage Policy, 6:00:00:00/5.

This policy applies to all faculty, staff, and students who use a mobile device owned by the College, or owned by the individual, which has access to the Southwest network or to retrieve or store sensitive College information. Vendors, contractors, or others who use mobile computing devices to access the Southwest network or to retrieve or store sensitive Southwest information may also be subject to this policy.

Mobile computing devices will be ordinarily deployed in three (3) ways:

1. As a resource assigned to an individual to replace a desktop PC, usually when an employee regularly works at more than one location.

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

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

Deployment Guidelines

1. 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 direct supervisor, Dean, or Director, and Information Technology Services. This form will accompany a fully approved Purchase Requisition form.

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 familiarity with the basic guidelines for securing the equipment, as well as an understanding of the obligations of mobile device use.

Mobile Computing Devices Ownership and Use Issues

1. If a laptop is requested to replace a standard desktop microcomputer, 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 Southwest policies and guidelines regarding software 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 must be encrypted with the College's encryption software before storing data on the device.

6. Systems are not to be modified in an attempt to circumvent security or the base installation as provided to the user by the College. If modifications to the device are required, then the user must consult with Information Technology Services.

7. Assigned devices are the property of Southwest and should not be utilized for personal gain or to violate copyright laws. This equipment may be monitored, and the College administration has the right to request the return of the equipment at any time.

8. Authorized device users may be held responsible for damage to, or loss of their assigned devices due to misuse, unauthorized use, negligence, or other conditions that the College finds are the fault of the user.

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 email, VPN, calendar events, etc. shall be protected by the lock codes provided by the device's operating system.

Use of the following guidelines will help minimize the theft risk of a College-issued mobile computing device and should be followed to the best of the user's ability:

1. Do not share an assigned device with any unauthorized user, especially if the device stores sensitive College information. It should be used exclusively by the authorized user.

2. Know where the device is at all times, as well as the hardware issued with it. Police officers agree that a laptop out of the authorized user's sight- even for a few seconds- is an easy mark.

3. Keep a 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 a thief to spot. A case containing the device should also be locked to provide an element of deterrence and delay.

4. Do not leave a device or accompanying hardware visible in an unattended motor vehicle. Lock the items in the trunk, when possible, store them on the floor of the vehicle out of sight, or cover the items so that they cannot be easily identified.

5. When a device will be left unattended, whether on campus or off campus, the door to the space should be locked. If possible, the device should be stored in a locked file cabinet or secured with a lock.

6. The case for the device should be identified in a unique way to make it stand out from all other bags. An unusual color, special large tags, or brightly colored objects attached to the bag will provide greater, immediate ability to locate the bag and give police probable cause to stop and question the carrier.

7. Clearly identify the device with a visible nametag on the bag and by writing your name, address, and telephone number on the case. Verify that the device has a Southwest 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.

8. While commuting in a taxi, shuttle bus, rideshare, or any type of public transportation, keep the device with you at all time. Do not permit the driver to load the device as baggage where it could be out of your view.

9. Keep the device with you as a carry-on piece when traveling. Placing it in the baggage compartment easily exposes it to the rigors of the baggage handling process and risks theft. Place the device in the under-seat storage area where you have more control, if possible, rather than in an overhead bin.

Owners or users of mobile computing devices that store sensitive College data must immediately report loss, theft, or suspected misuse of a device to Southwest Campus Police Services and to Information Technology Services.

Termination of College Relationship

All College-owned mobile devices must be returned to the Information Technology Services department upon termination of the assigned user's relationship with the College. Software applications purchased by the College and installed on a user's personal mobile computing device (not owned by the College), must be removed by the user immediately after separation from the College.

All users of Southwest computer and telecommunications resources are expected to read and abide by the College's Acceptable Usage Policy, 6:00:00:00/5.

Source of Policy: Information Technology

Responsible Administrator: Chief of Administrative Services

Related Policy: 6:00:00:00/5

TBR Policy Reference:

Approved: 
President

Date: July 1, 2024

Attachment A

SOUTHWEST TENNESSEE COMMUNITY COLLEGE

MOBILE COMPUTING DEVICES REQUEST

This form is intended to aid in assessing mobile computing devices needs

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:**_____

Additional hardware required: (check any that apply)

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

List additional hardware requirements

___ **Docking Station** ____ **Keyboard** ____ **Extra Batteries** **Other:**_____

Will the device contain student data? (yes/no) _____

Approximate number of hours per week unit will be used: _____

Will the requested device replace an another device: (yes/no) _____

Prepared By: _____ **Date:** _____

Dept. Head/Director: _____ **Date:** _____

Info Systems Representative: _____ **Date:** _____

Attachment B

SOUTHWEST TENNESSEE COMMUNITY COLLEGE

MOBILE COMPUTING DEVICES PERSONAL RESPONSIBILITY FORM

Name: _____ **Campus/Location:** _____

Department: _____

Equipment Description: _____

_____

_____

Equipment Serial Number: _____

Southwest Tennessee Community College asset tag number: _____

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.

I have read and understand the Security Guidelines in the Mobile Computing Devices Policy.

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

Signed: _____ **Date:** _____