


# PROCEDURE

<b>Subject:</b>	<b>IT Laptop and Mobile Devices</b>	<b>Number:</b> 2.60.06
<b>Source:</b>	Vice President, Planning and Institutional Effectiveness	<b>Reference (Rule #)</b> 6HX14-2.60
<b>President's Approval/Date:</b>	 4/10/18	

**PURPOSE:** This document outlines a set of practices and requirements for the safe use of State College of Florida (SCF) mobile devices.

**SCOPE:** This procedure applies to:

- Users, systems, and locations;
- Employees, contractors, students, service providers; and
- Applies to all facilities.

Personally owned devices (i.e., non-SCF owned) connect to environments that are segregated from systems containing sensitive data, and therefore are out of scope.

**POLICY STATEMENT:**

- 1.1 Laptops
  - a. Information Technology (IT) maintains a list of SCF laptops and has designed processes to maintain the security of these devices.
- 1.2 Portable Storage Devices
  - a. Portable storage (e.g., USB drives, CD ROM, DVD, SD cards) may not contain sensitive information (as defined in the SCF Data Classification Guidelines) without encryption.
  - b. All SCF mobile devices must be encrypted.
- 1.3 Mobile Device Technical Requirements
  - a. Devices must use an approved Operating Systems (OS); for example, Android (6.x Marshmallow or later) or IOS (9.1 or later).
  - b. Mobile devices, generally speaking, should not contain sensitive information.
  - c. Devices must store SCF user-saved passwords encrypted.
  - d. Devices must be configured with a secure password that complies with SCF Password Procedure.
  - e. College owned laptops must have full disk encryption.

- 1.4 User Requirements
- 1.5 Users may only load essential College data onto mobile device(s), as required to perform their work duties.
- 1.6 Users must report all lost or stolen portable devices that may contain sensitive information to IT Help Desk or your manager without delay.
- 1.7 If a user suspects that unauthorized access to College data has taken place via a mobile device, the user must report the issue in alignment with SCF Incident Response Procedures.
- 1.8 Devices must not have a compromised operating system (e.g., “jailbroken” or rooted access to the OS).
- 1.9 Users must not load pirated software or illegal content onto their devices.
- 1.10 Only formally IT approved software and applications may be installed on SCF devices.
- 1.11 Devices must be kept up to date with manufacturer or network provided patches. As a minimum, material patches should be updated monthly. SCF owned mobile devices must connect to the SCF wireless at least once every 30 days to receive updates.
- 1.12 Devices must be encrypted in line with SCF compliance standards.
- 1.13 Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that SCF data is only sent through the SCF email system. If a user suspects that company data has been sent from a personal email account, they must notify the Information Security Team (ITSecurity@scf.edu) immediately per the IT Incident Response Procedure.
- 1.14 Users must not use College workstations to backup or synchronize device content such as media files unless such content is required for legitimate business purposes.

**NONCOMPLIANCE:** Any employee/contractor found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. Service providers found to have violated this procedure may be subject to financial penalties, legal action, and including termination of contract.