Contents

PURPOSE: .............................................................................................................................................. 2
DEFINITIONS: ......................................................................................................................................... 2
BACKGROUND: ....................................................................................................................................... 2
REQUIRED MATERIALS AND SUPPLIES TO EXECUTE PROCEDURE: ............................................. 2
DELEGATION: .......................................................................................................................................... 2
PROCEDURE COMPLETION CRITERIA: .................................................................................................. 3
PROCEDURE: .......................................................................................................................................... 3
  Operation of Chapman University Computing and Storage Devices .................................................. 3
  Tracking Chapman University Computing and Specified Storage Devices ....................................... 3
  Remote Wipe ......................................................................................................................................... 3
  Acceptable Environmental Conditions for Use of Mobile Computing or Storage Devices Outside
  Campus Facilities ................................................................................................................................. 4
  Storage and Security of Chapman University-Owned Devices .......................................................... 4
Appendix A: ACCEPTABLE USE AUTHORIZATION - FORM ................................................................. 5
PURPOSE:

The intent of this standard is to describe Chapman University’s methodology for ensuring appropriate safeguards for the use and security of mobile computing and storage devices both in campus facilities and off campus as referenced in Chapman University Computer and Network acceptable use policy.

DEFINITIONS:

Sensitive Computing Devices: Magnetic Stripe Readers, Wireless Access Points, Handheld credit card devices, Smartphones, Tablets

BACKGROUND:

Chapman University must have a process for monitoring and distributing sensitive mobile computing and storage devices which may have impacts on important data.

REQUIRED MATERIALS AND SUPPLIES TO EXECUTE PROCEDURE:

Mobile Computing and Storage Device Acceptable Use - Form

DELEGATION:

1) Supervisors must authorize all use of mobile computing and storage devices by employees.

2) The Mobile Computing and Storage Device Acceptable Use Form (Appendix A) must be filled out by Supervisor and employee as designated in this standard.

3) Employees should only use mobile computing and storage devices in the execution of authorized work duties.

4) Employees must safeguard mobile computing and storage devices and any sensitive data stored/transmitted by them with the same protections afforded hardcopy sensitive documents of Chapman University.
PROCEDURE COMPLETION CRITERIA:

1) Mobile computing and storage devices must be approved by Supervisors and the DIS **Contact the Computing Services Manager for assistance**.

2) Prior to acquisition/distribution of said devices, completion of Sensitive Mobile Computing and Storage Device Acceptable Use Form (Appendix A) should be signed by the Approving Supervisor or Manager whom then will forward the completed authorization form to Director of Information Security (DIS) in IS&T for final approval.

PROCEDURE:

**Chapman University Owned Sensitive Mobile Computing and Storage Device Use**

**Operation of Chapman University Computing and Storage Devices**

a) Mobile computing and storage devices should be treated as any other Chapman University-owned equipment, used only by employees or student workers to execute work-related tasks as approved by management.

a) Alterations of hardware are prohibited. Should additions be made to the device, such amenities will become the property of Chapman University. Should IS&T elect to remove these additions, alterations, or improvements, IS&T reserves the right to charge a fee for the cost of restoring the device to its original configuration and condition. IS&T is not responsible for maintenance of or providing technical assistance for any non-standard applications or reconfigured hardware.

**Tracking Chapman University Computing and Specified Storage Devices**

a) Employee shall not remove or alter any identification labels that are attached to or displayed.

b) Chapman University documents information concerning checking out and tracking of mobile computing and specified storage devices. The Sensitive Mobile Computing Device and Software Acceptable Use - Form should denote the following:

i) Employee who will be using the device; Management approval; Item description and intended use; location, serial number, asset tag, make and model numbers.

ii) Mobile computing devices which are used as permanent or stationary workstations, with a single user, shall be exempt from this standard.

**Remote Wipe**

a) In the event of mobile computing devices being lost or stolen, DIS should be notified immediately. To report the incident, an incident report form must be filled...
out and submitted to DIS in the IS&T office. The incident report form can be found online at: http://www.chapman.edu/images/userImages/deterdin/Page_14634/CyberIncidentReportFormCHAPMAN.pdf

b) Chapman University is authorized to issue a remote wipe of your sensitive mobile device in the case it is lost or stolen and the item cannot be located.

Acceptable Environmental Conditions for Use of Mobile Computing or Storage Devices Outside Campus Facilities.

a) The mobile computing or storage device may not be left unattended in public areas.

Storage and Security of Chapman University-Owned Devices

a) When located within a campus facility, university owned mobile computing devices must be stored in locked file drawers, locked rooms, closets or cupboards, or locked down to the desktop.

b) Guidelines on reporting loss or theft of Chapman University property, including sensitive computing devices, are provided in Property Loss or Theft of Information Assets - Procedure.
Appendix A: ACCEPTABLE USE AUTHORIZATION - FORM

MOBILE COMPUTING AND STORAGE DEVICE
ACCEPTABLE USE AUTHORIZATION - FORM

By signing this form I acknowledge that I have read and agree to the Mobile Computing Device Standard and have had an opportunity to receive clarification as needed. I understand that if I leave employment with Chapman University or am no longer authorized to access Chapman University devices or data, I will return the computing or storage device, data and all accessories, including software and licenses to my supervisor.

Please Indicate Device Ownership
☐ Chapman University Owned Device
☐ Non-Chapman University Owned Device (Business or Institution is_______________________)
☐ Personally Owned Device

Agreed Upon By:

Employee Signature  Date

Printed Employee Name & Department

Supervisor or Manager Signature  Date

Print Supervisor or Manager Name & Department Here  Phone Extension

Authorized by:

Director of Information Security Signature  Date

Received by Name

*********************************************************STAFF ONLY SECTION*****************************************************************

Item Description, intended use, and location (include host computer info)  Serial Number/ Asset tag #  Make/Model #

*********************************************************STAFF ONLY SECTION*****************************************************************

Comments:

Form Distribution: IS&T (Palm 635) retains signed copy of form