UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Policy

Portable Computing Device Security

Purpose:

The purpose of this policy is to establish safeguards for the use of Portable Computing Devices (PCD) and their media in order to protect University data from unauthorized disclosure, use, modification, and loss.

Policy:

All OUHSC faculty, residents, fellows, staff, students and volunteers who use a Portable Computing Device to perform University Business are responsible for following these safeguards.

PCD includes but is not limited to laptops, notebook computers, tablets, smart phones (iPhones/Androids/Windows), cell phones, thumb drives, and external media such as CDs or DVDs. These safeguards apply to University-owned as well as personally-owned devices. See University Business definition below.

Safeguards:

1. **Inventory**: Each University department must maintain an inventory of PCDs used by its faculty, residents, fellows, staff, volunteers, and students to perform University business.

2. **Encryption:** PCDs used for University business must be encrypted to protect data from unauthorized disclosure if the device is lost or stolen.
    a. ALL laptops used for University business must be encrypted, regardless of who owns the laptop or of the operating system used.
    b. Encryption of laptops must be performed by department Tier Ones. This provides for centralized management and reporting for compliance purposes. See http://it.ouhsc.edu/services/infosecurity/LaptopEncryptionFAQ.asp.
    c. Residents, fellows, faculty, and staff who use their personally-owned laptops for University business are required to sign an agreement to have those devices encrypted in accordance with these safeguards.
    d. Smartphones and mobile devices used for University business must be enrolled in Secure Mobile. Secure Mobile enrollment is automated on mobile devices by establishing an ActiveSync connection with the OUHSC Exchange server (webmail.ouhsc.edu) for email synchronization. See http://it.ouhsc.edu/services/infosecurity/SecureMobileFAQ.asp.
    e. Only encrypted USB flash drives are to be used for University business.

3. **Password**: PCDs must require **user authentication, typically by requiring the user to enter a unique user-id and password (network login) or PIN**. If the PCD is not capable of using the University network password, then a local device or power-on passcode of at least four (4) digits or letters must be used. If a PIN is used, a local data wipe must be set to occur after 10 failed authentication attempts. Some devices provide biometric or user action (swipe) authentication. Users should check with the OUHSC IT Service Desk see if these alternative authentication methods meet requirements for the University resource used.

4. **Auto-Lock:** All PCDs must use an automated logoff (Auto-Lock) or password-protected screen saver that locks the device after a maximum of 15 minutes of inactivity. This ensures that the device will require a password entry if it is lost or left unattended.

5. **Manually Logoff**, lock, or power off the PCD when leaving it unattended so that a password will be required before allowing access.

6. **Storage of University Data:** PCDs should not be used to store University data unless required by business processes. University data should be stored on a server in the campus enterprise data center that provides appropriate physical security.

7. **Physical Safeguards:** Appropriate physical security measures must be taken to prevent theft of PCDs and media. PCDs must not be left unattended in vehicles or in public or unsecured areas.

8. **Wireless Transmission of Data:** Secure Wi-Fi networks that encrypt University data during transmission to or from a PCD must be used. On the OUHSC campuses, this is the "OUBASE" Wi-Fi network.

9. **Remote Access:** Approved remote access services and protocols must be used when transmitting University data. Most devices support using the Secure Portal at https://connect.ouhsc.edu/.

10. **Anti-virus: All** laptop computers must use a functioning and up-to-date anti-virus program. Virus programs should be set to automatically update definitions at least daily and to perform scanning on a weekly basis. All University owned laptops must use the centrally managed anti-virus platform as provided by the University's Information Technology Department. Antivirus protection must be used if available for other PCDs, such as smartphones, as the software becomes available, and as malicious code is developed for those devices. See http://it.ouhsc.edu/services/desktopmgmnt/antivirussoftware.asp.

11. **Lost or Stolen Devices:** Theft or loss of PCDs must be reported immediately to a supervisor, IT Information Security Services, and the University police. If the PCD stored PHI, the theft or loss must also be reported to the University Privacy Official and HIPAA Security Officer.

12. **Tracking:** It is recommended that users enable remote tracking capabilities such as "Find my iPhone" so they can find and/or remotely wipe lost or stolen devices.

13. **Disposal and Reuse:** PCDs users must follow the Information Technology Data Disposal and Reuse Policy and GreenSafe procedures to properly remove University data and software from a PCD before its disposal or reuse. Some devices can be restored to "factory defaults" to remove University data. Users should contact the IT Service Desk for assistance in resetting the device. Managers shall require that PCD users certify on the appropriate termination checklist that they have not retained any University data or software on their PCD or made or kept copies of data before separation from the University.

Scope:

This policy is applicable to all OUHSC faculty, residents, fellows, staff, or students who use PCDs for University business.

Regulatory Reference:

- HIPAA 45 CFR 164.308(a)(1)(ii)(B), 16 CFR Part 314, Standards for Safeguarding Customer Information
- Section 501(b) of the Gramm-Leach-Bliley Act ("G–L–B Act")
- GLB: 16 CFR Part 314 Standards for Safeguarding Customer Information
- State of Oklahoma Information Security, Policy Procedures Guidelines
- Payment Card Industry Data Security Standard (PCI DSS)

Definitions:

Portable Computing Device (PCD): includes but is not limited to laptops, notebook computers, tablets, smart phones (iPhones/Androids/Windows), cell phones, thumb drives, and external media such as CDs or DVDs.

University Business: Work performed as part of an employee's job responsibilities, or work performed on behalf of the University by faculty, staff, volunteers, students, other trainees, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University. University business includes the use of a Portable Computing Device to access OUHSC email, non-public University systems, networks, or data in the performance of work for the University.

	For additional Information Technology definitions, see Information Technology Policy Definitions Document at http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf.
Policy Authority/ Enforcement:	This policy is authorized and approved by the OUHSC Dean's Council and the Senior Vice President and Provost. Internal Audit may periodically assess Business Unit compliance with this policy and may report violations to the Board of Regents.

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
11/16/2005	1.0	OUHSC IT	Baseline Version
03/15/2013	1.1	OUHSC ISRB and IT	Mandatory encryption of all laptops and USB flash drives per memo from the Senior Vice President and Provost
10/21/2013	1.2	OUHSC ISRB and IT	Defining phases of implementation per memo from The Senior Vice President and Provost
10/07/2015	2.0	OUHSC ISRB and IT	Combined policy and standard and some items from FAQ into one document. Rearranged language in Purpose. Added University Business as a qualifier in the policy statements per memo from the Interim Senior Vice President and Provost. Added definitions for PCD and Univ. Business.

Table 2 Approval History

Version	Approval Date	Approved by:	Title:
1.0	11/16/2005	OUHSC Dean's Council	
1.1	03/15/2013	M. Dewayne Andrews, M.D.	The Senior Vice President and Provost
1.2	10/21/2013	M. Dewayne Andrews, M.D.	The Senior Vice President and Provost
2.0	11/11/2015	OUHSC Dean's Council	

Table 3 Review History

Version	Review Date	Reviewed by:	Title:
1.0	05/07/2010	OUHSC IT	
1.1	10/02/2012	OUHSC ISRB	
1.2	11/18/2014	OUHSC IT	
2.0	10/07/2015	OUHSC IT	
2.0	10/13/2015	OUHSC ISRB	