Portable Computing Device Security Policy

Current Version	Compliance Date	Approved Date
2.4	12/31/2018	11/13/2018

1. Purpose

This policy defines the requirements for appropriate use of portable computing devices, regardless of ownership, on the OUHSC network and the storage of intellectual property, regulated data, or University licensed software on those devices.

OUHSC employees, trainees, affiliates, volunteers, and any other user who uses the OUHSC network or computing resources for University Business and who wish to use Portable Computing Devices (PCD) for University Business must abide by this policy.

2. Scope

This policy applies to employees, trainees, affiliates volunteers, and any other user who utilizes the OUHSC network or computing resources provided by OUHSC for University Business with Portable Computing Devices, such as:

- Portable computers; e.g., laptops, notebooks computers, netbooks
- Portable storage media; e.g., USB storage devices, flash memory cards, CD/DVD ROM
- Mobile devices; e.g., smartphones, tablet computers, alphanumeric pagers

3. Policy

Employees, trainees, affiliates volunteers, and any other user who use Portable Computing Devices for University Business must comply with the following:

A. Risks, Liabilities, Disclaimers

Employees, trainees, affiliates and volunteers who elect to use their personal PCD for University Business accept the following risks, liabilities, and disclaimers:

- At no time does the University accept liability for the maintenance, backup, or loss of data on a Portable Computing Device. It is the responsibility of the owner or user to back up all software and data to other appropriate back-up storage systems.
- OUHSC will comply with applicable laws regarding data loss or breach notification and may also refer suspected violations of applicable laws to appropriate law enforcement agencies. Persons violating applicable laws or this policy may also be held personally liable for resulting damages and civil or criminal penalties.
- The University is not liable for the loss, theft, or damage of Portable Computing Devices. This includes, but is not limited to, when the device is being used for University Business, on University time, or during University travel.

- OUHSC reserves the right to implement and mandate technology such as disk encryption, anti-virus, and/or Mobile Device Management to enable or require the removal of OUHSC-owned data from personally-owned devices.
- Portable Computing Devices used for University Business may be subject to search and review as a result of litigation that involves the University, investigations related to the device owner's or user's activity, or other administrative purpose.

B. Security

OUHSC IT may perform security scans against any Portable Computing Device that accesses an OUHSC network, in accordance with the OUHSC Vulnerability Management Policy. IT may, without notification to the owner or user, prevent or ban Portable Computing Devices that disrupt any University computing resources, are used in a manner that violates any University policies, or that pose a risk to University systems or resources.

C. Safeguards

1. **Inventory**: Each University department, through its Tier One or IT representative, must maintain an inventory of PCDs used to perform University Business by the employees, trainees, affiliates, volunteers, and any other user in the areas they support. (See HIPAA Security Policy 3, Device and Media Controls, for inventory requirements.)
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 One/IT representative. This is required for centralized management and reporting for compliance purposes. See http://it.ouhsc.edu/services/infosecurity/LaptopEncryptionFAQ.asp.
    c. **Employees, trainees, affiliates, volunteers, and any other user who use their personally-owned Portable Computing Device for University Business may be required to sign an agreement to have those devices encrypted in accordance with these safeguards by Business Unit Information Technology staff.**
    d. **Smartphones and tablets 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 or contact your Tier 1/IT representative for assistance.
    e. Only encrypted USB flash drives that meet FIPS 140-2 Level 2 hardware-based and 256-bit Advanced Encryption Standard (AES) are permitted 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 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 must check with the OUHSC IT Service Desk to 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 the device is lost or stolen or left unattended.
5. **Users must manually logoff**, lock, or power off the PCD when leaving it unattended so that a password will be required to access the device.
6. **Storage of University Data:** PCDs should not be used to store University data unless required for University business processes. Local drives on computing equipment may not be used for storing

Category A or Category B data. Category A and Category B data must be stored on a server in the campus enterprise data center that provides appropriate physical security, unless other storage is required for business processes.

7. **Physical Safeguards:** Appropriate physical security measures must be taken to prevent theft of PCDs and media that contain University data. PCDs and media must not be left unattended in the passenger compartment of vehicles or in public or unsecured areas, for example.
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 "HSCACCESS" 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/, which will comply with this requirement.
10. **Anti-virus:** All laptop and desktop computers used for University Business must use a functioning and up-to-date anti-virus program. Anti-virus programs must be set to automatically update definitions at least daily and to perform scanning on a weekly basis by the IS Administrator. All University-owned laptops must use the centrally managed anti-virus platform as provided by the University's Information Technology Department. See http://it.ouhsc.edu/services/desktopmgmnt/antivirussoftware.asp.
11. **Antivirus protection** must be used if available for other types of PCDs, such as smartphones.
12. **Lost or Stolen Devices:** Theft or loss of PCDs must be reported immediately to IT Information Security Services and local law enforcement. If the PCD stored or may have stored PHI, the theft or loss must also be reported to the University Privacy Official or HIPAA Security Officer.
13. **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.
14. **Disposal and Reuse:** PCD users must follow the Information Technology Electronic Data Disposal and Reuse Policy) and 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 must contact the IT Service Desk or their Tier 1/IT representative for assistance in resetting the device.
15. Managers shall require that PCD users certify on the appropriate **termination checklist** that the users have not retained any University data or software on their PCD or made or kept copies of data before separation from the University.

4. Roles and Responsibilities

OUHSC Employees, Trainees, Affiliates, Volunteers, and any other user are responsible for the following:

- Registering their devices in the HSCAccess registration database. (This process must be repeated if devices are replaced or new devices are added.)
- Keeping security patches on devices up to date.
- Not removing or changing the encryption settings or device names? on devices used for University Business.
- Not storing protected data, such as PHI, PCI, PII, FERPA, or other confidential information on personally-owned computing devices.
- Destroying, removing, or returning all data - electronic or otherwise - belonging to OUHSC, once the employment, training, or volunteer relationship with OUHSC ends or once they are no longer the owner or only user of the personally-owned computing device.
- Removing or returning all software application licenses belonging to OUHSC when the device is no longer used for University Business.
- Notifying OUHSC IT Security of any theft or loss of a personally-owned computing device containing data or software application licenses belonging to OUHSC, as described above.

- Completing the appropriate termination checklist upon separation from the University, as described above.

5. Enforcement

This policy is authorized and approved by the OUHSC Dean's Council and the Senior Vice President and Provost and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University, including but not limited to Information Technology and the Office of Compliance, may periodically assess a user's compliance with this policy and may report violations to the department and University administration and the Board of Regents.

6. Regulatory References

- HIPAA 45 CFR 164.308(a)(1)(ii)(B)
- 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)
- HITRUST 09.o Management of Removable Media
- HITRUST 09.j Controls Against Malicious Code
- HITRUST 06.d Data Protection and Privacy of Covered Information

7. Definitions

See Information Technology Policy Definitions Document at
http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf.

8. Review Frequency

This policy is scheduled to be reviewed, updated and modified, at least every two (2) years, and more often as necessary.

9. Revision, Approval and Review

9.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	11/16/2005	OUHSC IT	Baseline Version
1.1	03/15/2015	OUHSC ISRB and Campus IT	Mandatory encryption of all laptops and USB flash drives per memo from the Senior Vice President and Provost
1.2	10/21/2013	OUHSC ISRB and OUHSC IT	Defining phases of implementation per memo from The Senior Vice President and Provost
2.0	10/07/2015	OUHSC ISRB and OUHSC 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.
2.1	10/31/2016	OUHSC IT	Combined the BYOD and PCD policy.

			Updated enforcement statement to include CIO.
2.2	11/18/2016	OUHSC IT	Updated FIPS 140-2 requirement in item 2.e.
2.3	04/03/2017	OUHSC IT Director of Information Security	Revised updates for personal devices
2.4	10/26/2018	OUHSC IT	Update scope to include “any other user”. Updated PCD definition to include alphanumeric pagers.

9.2 Approval History

Version	Date	Approved By
1.0	11/16/2005	OUHSC Dean’s Council
1.1	03/15/2013	M. Dewayne Andrews, M.D.
1.2	10/21/2016	M. Dewayne Andrews, M.D.
2.0	11/11/2015	OUHSC Dean’s Council
2.4	11/13/2018	Information Security Review Board

9.3 Review History

Date	Reviewed By
05/07/2010	OUHSC IT
10/02/2012	OUHSC ISRB
11/18/2014	OUHSC IT
10/07/2015	OUHSC IT
10/13/2015	OUHSC ISRB
10/31/2016	OUHSC IT
12/4/2016	Legal Counsel
12/5/2016	OUHSC IT