Information Technology Security Standards: Portable Computing Devices

UNIVERSITY OF OKLAHOMA
Information Technology
Security Standard

<table>
<thead>
<tr>
<th>Standards Title: Portable Computing Device Security</th>
<th>Coverage: OU Health Sciences Center and Health Care Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard #: Information Security S.9.8.1</td>
<td>Version: 1.5</td>
</tr>
<tr>
<td>Regulation: HIPAA, FERPA, GLB, PCI, NIST, State of Oklahoma</td>
<td>Approved: 11-15-2005</td>
</tr>
</tbody>
</table>

Standards:

All Portable Computing Devices (PCDs), irrespective of device ownership, that connect to non-public university information resources must follow University policies and standards for the security of these resources. This includes PCDs that access University email systems.

PCD includes but is not limited to laptops, notebook computers, tablet PCs, smart phones, cell phones, thumb drives and external media such as CDs or DVDs.

1. **Password protection:** Any computing device that accesses non-public University information systems must require user authentication, typically by requiring the user to enter a unique user-id and password. If the PCD is not capable of using the University network authentication method, then a local device or power on password must be used. Some devices provide biometric or user action (swipe) authentication. Check with university PCD device security standards to see if these alternative authentication methods meet requirements for the university resource you use.

2. Enable 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 lost or left unattended.

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

4. **Storage of sensitive information:** PCDs should not be used to store sensitive information unless required by business processes. In the case of storage requirements, all data must be encrypted. Sensitive data should be stored on a server in the campus enterprise data center that provides appropriate physical security.

5. **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 the operating system used.
   b. Encryption of laptops must be performed by department tier ones.
   c. Residents, fellows, faculty and staff who use their personally-owned laptops for University business will be required to sign an agreement to encrypt those devices.
   d. Only encrypted USB flash drives are to be used for University business.

6. **Transmission:** Users shall not use their PCD to transmit sensitive information unless required by business processes and all transmissions are encrypted.
7. **Physical safeguards**: Appropriate physical security measures should be taken to prevent theft of PCDs and media. Unattended PCDs and media must be physically secure.

8. **Theft**: 
   a. **Reporting**: Theft of PCDs used for University business must be reported immediately to your supervisor, IT Information Security Services and the University police;  
   b. **Remote data delete**: It is recommended to remotely wipe the device in the event of loss or theft;  
   c. **Tracking**: It is recommended that PCDs use remote tracking capabilities;

9. **Wireless**: Approved wireless transmission protocols and encryption must be used when transmitting sensitive information. Sensitive data traveling to and from the PCD must be encrypted during transmission.

10. **Remote Access**: Approved remote access services and protocols must be used when transmitting sensitive information. *(See Remote Access Standard)*

11. **Disposal and Reuse**: PCDs users must follow the *Data Disposal and Reuse Policy* to properly remove data and software from the PCD before its disposal or reuse. Upon the revocation of PCD use authorization and/or voluntary or involuntary termination, PCD users shall certify that they have not retained any sensitive data on their PCD or made or kept copies of sensitive data.

12. **Antivirus**: Laptop computers must use an approved, functioning, and up to date antivirus program as provided by the University. Antivirus protection must be used if available for other PCDs as the software becomes available and as malicious code is developed for those devices.

The University reserves the right to audit PCDs to ensure that users are meeting the requirements of all University policies and standards. This includes, but is not limited to the right to review the information stored on PCDs. PCD users found to be in violation of University policies and standards related to PCDs shall be subject to revocation of their access to University information systems from their PCD.

**Scope/Applicability:** This standard is applicable to OU Health Sciences Center and Health Care Components and affects all staff that has responsibility for maintaining a portable computing device.


**Responsibilities:** Users are responsible for the security of PCDs they use for university business purposes.

**Definitions:** *Portable Computing Device (PCD)*: includes but is not limited to laptops, notebook computers, tablet PCs, smart phones, cell phones, thumb drives and external media such as CDs or DVDs. For more definitions, see: "IT Security Policy Definitions"
Procedures: Each department that maintains information systems and electronic media is responsible for developing procedures to comply with these standards.