UW - Department Family Medicine
Laptop Appropriate Use Policy

1.0 Policy Name
Department of Family Medicine (DFM) Laptop Appropriate Use Policy

2.0 Definition and Purpose
This policy outlines appropriate use of departmental laptops, approved configurations and expected employee or guest behavior regarding the use of laptop computers. This policy is intended to augment and complement the UWHealth Acceptable Use Policy. (Please visit https://www.uconnect.wisc.edu for a copy of this policy)

3.0 Scope of Policy
This policy applies to Department of Family Medicine employees or guests utilizing laptop computers owned and operated by the Department of Family Medicine as well as any laptop computer connecting (either directly or through a wireless method) to UWHealth networks or UWHealth shared resources.

4.0 Policy Statement

4.1 Laptop Network Connections

a. A personally owned laptop may not be physically or wirelessly connected to DFM/UWHealth private networks due to security reasons.
b. Laptops connected to a DFM/UWHealth network must meet ALL of the following criteria:
    1. Purchased with DFM funds, UWMF, UWHealth funds, and/or grant funds.
    2. Meet pre-approved technical specifications as designated by DFM ITS staff.
    3. Hardware encryption enabled and active with bios-level password protection enabled.
    4. Configured by DFM ITS staff according to standard OS and Application images.
c. A DFM wireless network must be authorized, configured and supported by DFM ITS.
d. Personal laptops may be connected to an authorized UWHealth public wireless network. An authorized UWHealth public wireless network is configured and managed by UWHealth IT Services.
e. DFM ITS will provide limited support in connecting personal laptops to a UWHealth authorized public wireless network. DFM ITS will not provide support for personally owned wireless networks nor for a hot spot WIFI connection.

4.2 Laptop Configurations

a. To ensure HIPAA compliance and compliance with UWHealth policies, DFM laptops are required to run the following security software at all times. Security software configurations and Operating Systems MAY NOT be altered or removed by the employee or guest.
b. Disabling or removal of any of the systems listed constitutes a breach of this policy as well as a breach of UWHeath Acceptable Use Policy and may result in HR action against the employee.
c. DFM laptops will be processed by an initial audit process at the time of installation and/or deployment. Periodic audits will be performed to ensure compliance with Policy.
d. Required software list:
    1. Firewall Protection
    2. Anti-Virus Protection
    3. Spyware Protection
    4. System Updates
    5. Hardware Disk Encryption with bios-level password
    6. Altiris management client

4.3 Updates

a. Employees using a DFM laptop are expected to routinely connect their laptop to a network (DFM network or home network) to receive timely operating system and security updates.
b. For major software updates, DFM users may be asked to return their device to the DFM Help Desk in Alumni Hall for maintenance.
c. Employees may be asked to leave their laptops connected to the network and turned on at a clinical location for maintenance or troubleshooting purposes.

4.4 Screensavers

a. Laptops will have a password-protected screensaver activated after 15 minutes of idle usage.

4.5 Installing Software

a. Employees using a DFM laptop will have limited administrative rights to the device.
b. Employees using a DFM laptop are expected to install only work-related software. Examples of inappropriate software to install on DFM laptop include (but are not limited to) games, wallpaper, weather notifications, and/or file sharing services.
    a. Any software discovered during regular maintenance or an audit that is deemed to be non-work-related will be immediately removed either by an automated maintenance process or by DFM IT staff.

4.6 Data Backup

a. Employees using a DFM laptop should routinely back-up files stored on their laptop to the UWHealth network or another storage source to reduce the risk of lost data. For assistance with a laptop backup solution, please contact the DFM Help Desk.
b. To streamline troubleshooting problems with laptops, the DFM Help Desk will complete initial troubleshooting steps with a laptop and if unsuccessful in resolving the issue, the DFM Help Desk will erase the hard drive and reinstall a new standard image onto the laptop hard drive.
c. After the re-image process, the laptop will not contain any data that was previously stored on the laptop, such as, bookmark favorites, Mobile Device data, PowerPoint files, Word files, Excel files, and/or any other personal settings that were previously stored on the laptop.
    a. DFM IT Staff will not back up personal files or assist in the recovery of personal files of any kind.

4.7 PHI (Protected Health Information)

a. Access to PHI requires UWHealth-authorized credentials to PHI-based systems.
b. As a general rule, PHI should not be stored directly on the hard drive of a laptop. PHI should be stored on a UWHealth server. However, if PHI needs to be stored on a laptop, encryption software that has been approved by the DFM Help Desk is required.

4.8 Employee Accountability and expectations

a. Employees are expected to return laptop devices to the DFM Help Desk on request within a reasonable time frame for any reason.
b. Employees utilizing a DFM-owned laptop are expected to follow standard security practices (as outlined by UWHealth policies), maintain possession of the laptop at all times, and report lost or stolen devices to DFM Help desk immediately.
c. Consistent with UW-Madison Appropriate Use Policy and UWHealth Acceptable Use Policy, violations of this Policy may lead to the suspension of computer access privileges pending investigation of circumstance. Serious violations of this policy will be referred to the Employee or Guest's supervisor and/or DFM Human Resources. Unacceptable use of any DFM technology resource could result in penalties as severe as termination of employment and/or criminal prosecution. Depending on the offense, violators may be subject to prosecution under State and/or Federal laws.

Implementation Date	October 17th, 2013
Last Revision Date	9/22/13