Wireless Access Security Standard

1. Purpose

The purpose of this *Wireless Access Security* Standard is to provide OUHSC personnel, faculty, staff, and students with notice of the minimum security requirements that must be in place in order to use personally-owned or University-owned devices to access the University-provided business wireless network.

2. Standard

All devices that will be used to access the HSCACCESS wireless network must comply with the following minimum security requirements, as confirmed by the device user's Tier One, Service Desk or IT Representative:

- All devices must be registered in accordance with the HSCACCESS Registration Process, described in the "Related Documents" section below.
- Laptops must have an up-to-date version of the McAfee ePO agent installed.
- ePO clients must remain in a "Managed State."
- Laptops must have an up-to-date version of McAfee Drive Encryption or Management of Native Encryption or Dell Data Protection full drive encryption installed and be registered as encrypted with the respective management server
    - ePO encryption must report as "Enabled" or "Active."
- Laptops must have up-to-date version of McAfee Enterprise VirusScan installed.
    - McAfee Enterprise VirusScan must be configured to update virus definition files on at least a daily basis and to perform scans on at least a weekly basis.
- Laptops must have either McAfee File and Removable Media Protection or Dell Data Protection (External Media Shield) installed and functioning to encrypt removable media.
- Laptops used on the OU-Tulsa campus must have the Global Protect client installed and configured.
- Laptops used on the OUHSC OKC campus and clinic locations must have the Pulse Secure client installed and configured.
    - The laptop user must be assigned membership to at least one UAC security group, as assigned by their Tier 1, Service Desk or IT Representative.

    NOTE: Users should contact their Tier 1s or IT Representatives for assistance in registering their devices.

- Smart phones and tablets must be configured to adhere to the following security requirements:
    - **Device Passcode** – A passcode setting of at least four (4) numbers or letters must be set. Smartphone users are responsible for setting and remembering their device passcode. OUHSC technical support will not be able to recover a forgotten passcode on a Smartphone. The user may have to reset the device to factory defaults and may lose all locally- stored data if the user forgets the passcode and has not backed up the data.

- **Encryption of Data Stored on the Device**- An industry standard encryption mechanism must be implemented for all data stored locally on the device, including removable media and backups.
- **Password-Protected Screen Saver** – A password-protected screen saver must be configured to automatically lock the screen after a maximum of fifteen (15) minutes of inactivity and must require a passcode to unlock the device.
- **Local Data Wipe for Failed Login Attempts**– A setting that implements a local data wipe after 10 failed authentication attempts must be enabled.

NOTE: Users may meet the smart phone security requirements, in most cases, when they sync their smartphones to the University's email systems. Users should contact their Tier 1s, Service Desk or IT Representatives if they need assistance.

3. Related Documents

- Knowledge base article: Device registration process for access to HSCACCESS Wi-Fi network.
- Knowledge base articles for tier ones (IT) detailing procedures to configure endpoints for HSCACCESS Wi-Fi.
  - Go to https://help.ouhsc.edu and search for the specific topic, i.e. "HSCACESS"
- OUHSC Business Services that require HSCACCESS
  - https://ouitservices.service-now.com/kb_view.do?sysparm_article=KB0011443 (OUHSC OKC)
  - https://outulsa.service-now.com/kb_view.do?sysparm_article=KB0010606 (OU-Tulsa)
- OUHSC Services that Require HSCSTUDENT
  - https://ouitservices.service-now.com/kb_view.do?sysparm_article=KB0011464
- Portable Computing Device Security Policy
  - http://it.ouhsc.edu/policies/PortableDeviceSecurityPolicy.asp

4. Scope

This Standard is applicable to all OUHSC faculty, residents, fellows, staff, and students who use OUHSC's HSCACESS wireless network.

5. Revision, Approval and Review

5.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	10/19/2016	Campus IT	Baseline Version
1.1	11/30/2016	D Saliba, Tulsa IT	OU-T IT specifics

5.2 Approval History

Version	Date	Approved By
1.0	11/08/2016	OUHSC Information Security Review Board

5.3 Review History

Date	Reviewed By