Workstation Baseline Security Configuration Standard

Current Version	Compliance Date	Approved Date
1.5	05/31/2018	05/08/2018

1. Purpose

The purpose of the Workstation Device Baseline Security Configuration Standard is to provide a baseline security configuration to address cybersecurity vulnerabilities for workstations used to perform University Business. OUHSC requires workstations used to perform University Business to meet minimum security requirements in order to protect the confidentiality, integrity, and availability of University information systems and data.

2. Standard

All OUHSC workstations used to perform University Business must be configured by the IS Administrator to meet the minimum security baseline listed below.

Active Directory

- All University-owned and University-leased workstations that are compatible with Microsoft Active Directory
 (AD) must be added as members to the appropriate departmental AD Organizational Unit (OU) under the
 HSC.NET.OU.EDU\WORKSTATIONS OU.
 - 1. Example: HSC.NET.OU.EDU\WORKSTATIONS\Dentistry\Laptops\OUHSC
- b. All University-owned and University-leased workstations must be named according to the following naming scheme to aid in identification.
 - 1. [College][Department or Building][Serial_Number or Service Tag]
 - i. Example: ITROBMPHYY72
- c. All University-owned and University-leased workstations must be configured to display the following login banner:

"This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system or in the course of system maintenance the activities of authorized users may also, be monitored. Anyone using this system expressly consents to, such monitoring and is advised that if such monitoring reveals, possible criminal activity or policy violation system personnel may, provide the evidence of such monitoring to law enforcement or other officials.."

- d. The "Managed by" field of the Organizational Unit in AD must be populated with the Active Directory Username for the IS Administrator.
- e. All workstations must have the "Domain Admins" group as a member of the local "Administrators" group.

Device Lock/Logoff Policy

a. All IS must be secured with either a password-protected screen saver or automatic logoff that will take effect after no more than fifteen (15) minutes of inactivity.

Logging

a. All IS must be configured to retain Information System log data in accordance with the *Information System Logging and Review Policy*.

Anti-Virus

- a. All IS, where supported by the operating system or vendor, must use the centrally managed anti-virus platform provided by OUHSC Information Technology.
- b. Anti-virus software must be enabled, running, and up-to-date.
- c. Anti-virus software must be configured to perform a full anti-virus scan weekly.
- d. All IS anti-virus platforms must check for updates on a daily basis.
- e. Faculty, staff, and students/trainees who use personally-owned IS for University Business must first register the IS and be configured for use by OUHSC Information Technology via the Secure Network Access Program (SNAP). IS Administrators may be contacted for assistance with this requirement.

Encryption

All workstations at off-premise clinical locations must be encrypted. (Off-premise clinics are those locations which are not on the primary Oklahoma City or Tulsa campuses. For a list of off-premise clinic locations see the Office of Compliance.)

Vulnerability and Patch Management

- a. All workstations must be running current and supported version of its operating system.
- b. All workstations must have an assigned IS Administrator responsible for patch and vulnerability management of all hardware and software.
- c. All workstations must adhere to the OUHSC Patch Maintenance schedule, available from https://it.ouhsc.edu/policies.
- d. All workstations must undergo a regular vulnerability scan in accordance with the OUHSC Vulnerability Management Policy and Standard, performed by the IS Administrator.
- e. Before leaving a workstation unattended, even briefly, users must lock or logoff the workstation to prevent unauthorized access.
- f. IS Administrators must configure workstations to be secured with a password-protected screen saver or automatic logoff that will take effect after no more than 15 minutes of inactivity.
- g. All workstations, regardless of ownership, must be documented in the departmental asset inventory system of record, maintained by the IS Administrator.

Unsupported Operating Systems

- a. Mac OSX 10.10.x and below
- b. MS Windows XP
- c. MS Windows Vista
- d. MS Windows 95
- e. MS Windows 98
- f. Windows NT Workstation 4
- g. MS Windows ME

3. Related Documents

- Access to Sensitive Data Policy
- Antivirus Policy
- Business Unit Roles and Responsibilities Policy
- Password Management Policy
- Transmission of Sensitive Data Policy
- Vulnerability Assessment Policy

4. Scope

All staff, faculty, residents, students, guests, third parties, and other entities connecting workstations to the OUHSC network or non-public Information System are subject to this standard.

5. Revision, Approval and Review

5.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	10/6/2016	OUHSC IT	Baseline Version
1.1	11/3/2016	OUHSC IT	Added Active Directory membership requirements.
1.2	11/29/2016	Randy Moore	Modified introduction to replace "connection to the network" with "University business". Specified AD OU. Added "When Leaving a workstation unattended".
1.3	01/19/2018	April Lee	Unsupported Operating Systems
1.4	03/26/2018	Subject Matter Experts	Minor revisions
1.5	5/07/2018	Randy Moore	Added section for encryption of desktops at remote clinics

5.2 Approval History

Version	Date	Approved By
1.5	05/08/2018	Information Security Review Board

5.3 Review History

Date	Reviewed By	
05/08/2018	Information Security Review Board	