POLICY INFORMATION

Document # **3000**	Title: **Workstation Use & Security**	Print Date: **8/08/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Physical**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7AB6B86710B5491...	Date Approved: 8/29/2016

I. POLICY STATEMENT

This policy shall establish minimum requirements for the implementation of physical safeguards for workstations that access confidential information within CEHS Health Care Components (HCC) in order to maintain the confidentiality, integrity, and availability of CEHS electronic information and information systems.

II. DEFINITIONS

See HIPAA Privacy Policy 100

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the Health Care Component (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

It is the policy of CEHS that logical and physical safeguards must be implemented for workstations that access sensitive or restricted information to restrict access to authorized users. The safeguards include processes that define how workstations may be utilized for accessing information as well as physical attributes of the surroundings of workstations.

Workstation Use:

1. **Power-on and Screen Saver Passwords:**
    a. All workstation access must be through user authentication.
    b. Password protected screen savers should be invoked by users when workstations are left unattended to deter unauthorized users.
    c. Screen saver activation intervals should be short in length (e.g., 5 to 15 minutes). The time interval should be determined based upon the location and accessibility to the workstation.

2. **Password Standards:**
    a. Passwords must be unique and have a minimum of eight characters with at least one alphabetic character and one numeric character.
    b. Passwords must be secure at all times. They must not be written and stored in an accessible location.
    c. Passwords must not be shared under any circumstances.
    d. Users are responsible for maintaining the confidentiality of their passwords. Any inappropriate use of a password will be the user's responsibility and could be subject to disciplinary actions and sanctions under the CEHS Sanctions Policy 201 and any USU Human Resource policies that are applicable.
    e. Users are not allowed to use data under another person's account that has been logged into a system.
    f. Users shall not observe the password entry of other users and shall make reasonable effort to prevent others from observing their password entry.

3. **Inactivity Timeouts and Manual Log-off:**
    a. Inactivity time-outs shall be enforced for workstations that access restricted, sensitive and confidential information such as EPHI. This time-out functionality should clear the workstation screen and close access to confidential or sensitive electronic information, including EPHI after a defined period of inactivity (e.g., 5 to 15 minutes).
    b. Users will log-off or place workstations in a secure or locked status whenever leaving it unattended.

4. **Offsite Computers:**
    a. Equipment containing confidential or sensitive electronic information, including electronic protected health information (EPHI), should not be taken off-site without documented authorization. Where appropriate, equipment and /or software should be checked out and back in when returned.
    b. CEHS owned equipment (including workstations) may only be used by the individuals approved to use it.

5. **Unauthorized Software:**
    a. Documented management approval is required for acquisition of all software.
    b. Prior to purchase an Inherent Risk Assessment must be performed on the system with the Security Officer.
    c. All software must be legally obtained, approved by the CEHS Security Officer, appropriately licensed and screened for viruses before installation.
    d. Audits of workstations to ensure unauthorized software has not been installed will be performed on a periodic basis.

6. **Acceptable Use:**
    a. Users must not save on workstations information classified Confidential, Private, or otherwise considered sensitive or privileged information, unless it is appropriately secured against theft or loss.
        i. Users and HCC should consult with their system administrator and the CEHS Security Officer regarding what kind of security is appropriate for the sensitive information they store on their local workstations.
    b. All personnel shall be responsible for protecting the information resources at individual workstations and abiding by all Security Policies and Procedures that apply to their individual environment.
    c. Workstations connected to critical business applications should be purchased with the help of the Security Officer or the HCC unit's assigned system administrator. The workstations shall be tested prior to use, supported by effective maintenance arrangements and protected by appropriate physical controls.
    d. Users must backup critical data according to the security plan

7. **Workstation Configurations:**
    a. CEHS Security Officer is responsible for defining base controls and configurations for workstation builds. HCC unit system administrators are responsible for maintaining and inventorying each workstation/electronic device and documentation of systems used on each workstation and are responsible to incorporate the baseline security controls, safeguards and configurations into their workstation builds.
    b. Only authorized personnel (e.g., system administrator, Security Officer) are permitted to perform workstation configurations.
    c. Workstation configurations or procedures should prevent users from:
        i. Installing unauthorized software
        ii. Modifying system configuration files
        iii. Modifying access control lists for systems files and other people's user files
        iv. Accessing games except where authorized by the system administrator
    d. Each workstation is required to be protected from malicious software by up-to-date anti-virus software or an appropriate and effective alternative. This shall be determined by the Security Officer.

Workstation Security:

1. Workstations will be located in secure locations based on reasonableness of functions performed.
2. Workstations used infrequently will be located in a secure area or locked when not in use.
3. Doors leading into offices with desktop/laptops should always be locked when vacated.
4. Workstations that provide access to or use of sensitive information or information systems should not be located in publicly accessible areas.

   a. If a workstation must be located in a public area, physical and technical safeguards must be employed to protect against unauthorized access such as security locking cables or cages.
5. All workstation monitors are to be positioned in a way that prevents casual viewing by unauthorized users and the general public.
6. Users must ensure that all devices and media used at the workstation location are secured.

Monitoring and Auditing:

1. CEHS Security Officer will monitor the Workstation Use and Security standards for compliance and changes, and update CEHS processes and procedures as necessary.
2. The workstation controls addressing the installation of unauthorized software will be monitored by the system administrator.
3. Violations will result in appropriate action based on the CEHS Sanctions Policy 201 and applicable USU Human Resources policies.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR §164.310 (b), (c)

CEHS Administrative Sanctions Policy 201

USU Policy 311