Workstation Security Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose
The purpose of this policy is to provide guidance for workstation security for <Company Name> workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

2.0 Scope
This policy applies to all <Company Name> employees, contractors, workforce members, vendors and agents with a <Company Name>-owned or personal-workstation connected to the <Company Name> network.

3.0 Policy
Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, including protected health information (PHI) and that access to sensitivity information is restricted to authorized users.

3.1 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.
3.2 <Company Name> will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.
3.3 Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitivity information, including protected health information (PHI) on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitivity information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the Portable Workstation Encryption policy
- Complying with the Anti-Virus policy
- Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents

- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the Wireless Access policy

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Workstations include: laptops, desktops, PDAs, computer based medical equipment containing or accessing patient information and authorized home workstations accessing the <Company Name> network.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of <Company Name>

6.0 Revision History