Workstation Security (For HIPAA) Policy

1.0 Purpose

The purpose of this policy is to establish security standards and provide guidance for the use of all workstations accessing organizational resources. The objectives are to ensure the confidentiality, integrity, and availability of information processed or accessed by workstations, including sensitive data such as Protected Health Information (PHI). This policy also aims to ensure compliance with relevant regulatory requirements, such as the workstation security standards mandated by the HIPAA Security Rule (164.310(c)), where applicable.

2.0 Scope

This policy applies to all employees, contractors, workforce members, vendors, and agents of the organization utilizing any workstation (whether organization-owned or personally-owned) that connects to the organization's network or is used to access, process, or store organizational information.

3.0 Policy Statements

All individuals subject to this policy must adhere to the following workstation security requirements:

3.1 General Security Awareness and Responsibility

* Users must always consider the sensitivity of the information being accessed or displayed on their workstation, particularly PHI or other confidential data, and take active steps to prevent unauthorized viewing or access.
* Workstations are provided for authorized organizational business purposes only. Personal use should be minimal and comply with the Acceptable Use Policy.

3.2 Access Control and Physical Security

* Workstations must be physically positioned and secured to minimize the risk of unauthorized access or viewing of sensitive information. Consider the use of privacy screen filters or other physical barriers where appropriate.
* Physical access to workstations must be restricted to authorized personnel only.
* Workstations must be secured (e.g., screen locked or logged out) whenever the user leaves the immediate vicinity, even for brief periods.

* A password-protected screen saver with a short inactivity timeout period must be enabled. Passwords must comply with the organization's Password Policy.
* Laptops containing sensitive information must be physically secured when unattended, using methods such as cable locks or storing them in locked drawers or cabinets.

3.3 Technical Safeguards and Configuration

* All workstations must comply with the organization's Baseline Workstation Configuration Standard.
* Only organization-approved software may be installed on workstations. Installation of unauthorized software is strictly prohibited.
* Sensitive information, including PHI, should primarily be stored on designated, secure network servers, not local workstation drives, unless explicitly permitted and adequately protected (e.g., through encryption).
* Workstations must comply with the Portable Workstation Encryption Policy, ensuring sensitive data stored locally is encrypted.
* Workstations must utilize appropriate power protection, such as a surge protector or an uninterruptible power supply (UPS/battery backup).
* If wireless network access is used, it must adhere to the security requirements outlined in the Wireless Communication Policy.

3.4 User Practices

* Keep food and liquids away from workstations to prevent accidental damage.
* Before leaving for extended periods (e.g., end of day), users should exit running applications and close open documents where practical, and ensure the workstation is left powered on but logged off to facilitate necessary after-hours maintenance and updates by IT personnel.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team) will verify compliance with this policy through various methods. These may include, but are not limited to, periodic physical inspections (walk-thrus), review of system logs and configuration settings, security audits (internal and external), and analysis of reports from security tools. Feedback will be provided to the policy owner and relevant management.

4.2 Exceptions

Any exception to this policy requires formal, documented justification and advance approval from the designated IT authority (e.g., Precision Computer team).

4.3 Enforcement

Failure by any individual subject to this policy to adhere to its requirements may result in disciplinary action, up to and including termination of employment or contract, consistent with

organizational procedures. Access privileges may also be modified or revoked.

5.0 Related Policies and Standards

Users should familiarize themselves with the following related organizational documents:

* Acceptable Use Policy
* Password Policy
* Portable Workstation Encryption Policy
* Wireless Communication Policy
* Baseline Workstation Configuration Standard
* Data Classification Policy (Implied reference via "sensitive information")

Revision #2
Created 28 August 2024 16:47:07 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery