SILICON VALLEY
CLEAN ENERGY

ITP14

Category: INFORMATION TECHNOLOGY

WORKSTATION SECURITY (For HIPAA) POLICY

I. PURPOSE

The purpose of this policy is to provide guidance for workstation security for SVCE workstations to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidelines to ensure the requirements of HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

II. SCOPE

This policy applies to all SVCE employees, contractors, vendors and agents with an SVCE-owned or personal workstation connected to the SVCE network.

III. POLICY

A. GENERAL

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and access to sensitive information, included protected health information (PHI), is restricted to authorized users.

SVCE will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Appropriate measures include:

- Securing file cabinets to restrict physical access 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. The password must comply with the SVCE Password Policy.

- Never installing unauthorized software on workstations.
- Storing all sensitive information, including PHI on network servers.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exiting running applications and closing open documents after use.
- Ensuring all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- Securing laptops that contain sensitive information by using cable locks or locking laptops in drawers or cabinets.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The IT Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

B. NON-COMPLIANCE

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