Workstation Security Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to implement physical safeguards for all workstations that access sensitive information and to restrict access to authorized users.

Scope:

This policy applies to all <<Organization name>> workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information by <<Organization Name>>. In addition, this policy applies to all workstations and other computing devices owned or operated by <<Organization Name>> and any computing device allowed to connect to <<Organization Name>>’s internal network.

Policy:

Physical safeguards will be implemented for all workstations that access sensitive information to restrict access to authorized users only.

All members of the workforce will be trained on the appropriate and authorized use of workstations as part of the security awareness training.

Workstations will be positioned such that the monitor screens and keyboards are not within view of unauthorized individuals.

Users will logoff prior to leaving the workstation. Users will store any written passwords in secure locations only – under no circumstance must any password information be accessible on the workstation or its vicinity.

Workstations must be labeled to identify function and location and assist with compliance with access control procedures.

All workstations must be operated in a manner that ensures:

* Confidentiality of sensitive information.
* Display of an appropriate warning banner prior to gaining operating system access.
* Employment of a password protected screen saver and/or workstation locking mechanism when the workstation is unattended.
* Proper log off and shut down of workstations at the end of the business day.
* Routine back up of all critical data.
* Virus scanning of media prior to use on any workstation.
* Only approved software may be used on <<Organization Name>>’s systems.
* Workstations and said software is used in accordance with contract agreements and copyright laws.

Responsibilities:

All individuals identified in the scope of this policy are responsible for:

* Using <<Organization Name>> computing devices only for work related purposes
* Following all procedures implemented by the Security Officer related to this policy.

The <<Organization Name>> Security Officer is responsible for:

* Maintaining procedures required to support this policy
* Supporting and ensuring compliance by workforce members

Compliance:

Failure to comply with this or any other security policy will result in disciplinary actions as per the HR XXXXX Policy. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

Procedure(s): None

Form(s): None

References:

* The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
* International Standards Organization (ISO 27002).

Contact:

John Doe, Security Officer

1234 Anystreet

Anywhere, WY XXXXX

E: John.doe@anywhere.com

P: 307.XXX.XXXX

F: 307.XXX.XXXX

Policy History: Initial effective date: July 1, 2015