



WORKSTATION SECURITY POLICY

PURPOSE

The purpose of this policy is to provide guidance for the security of computer workstations operated by The Early Learning Coalition of Pasco and Hernando Counties, Inc. (hereafter the “Coalition”) in order to ensure the security of information on the workstation and information to which the workstation may have access. Additionally, the policy provides guidance to ensure the requirements of the HIPPA Security Rule “Workstation Security” Standard 164.310(c) are met.

SCOPE

This policy applies to all employees of the Coalition, its contractors, vendors and agents with a personal-workstation connected to the Coalition network or Enhanced Field System (EFS) database.

POLICY

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected personal information and that access to sensitive information is restricted to authorized users.

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

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 sensitive information, including personal information on network servers.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- 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).

- Mobile computing devices may not be removed from the premises prior to receiving Management approval. Mobile devices being utilized outside office premises will be tracked by the Office Manager.
- Remote access must be approved by the Executive Director or Assistant Executive Director. Remote access may be monitored by IT contractor upon request.

ENFORCEMENT

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

DEFINITIONS

Workstations: laptops, desktops, PDAs, computer based equipment containing or accessing information and authorized home workstations accessing the Coalition network.

1st Reading: March 24, 2010

Approved by Board of Directors: May 27, 2010

Amended and Approved by Board of Directors: January 27, 2011