CAMPASPE COLLEGE of Adult Education Echuca

RISK MANAGEMENT
COMPUTER WORKSTATION SECURITY
8.12

Policy Rationale
The purpose of this policy is to provide guidance for workstation security for CCAE workstations in order to ensure the security of information on the workstation and information the workstation may have access to.

Policy Aims
This policy applies to all CCAE employees, contractors, workforce members, vendors and agents with a CCAE owned or personal-workstation connected to the CCAE network.

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

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of CCAE.

Procedure – Workstation Security
Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information and that access to sensitivity information is restricted to authorised users.

Workforce members using workstations shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.

CCAE will implement physical and technical safeguards for all workstations that access electronic 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 sensitivity information 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 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 updated with the system vendors security and patches.
- 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 applying a Wireless Access policy

Procedure – Workstation Settings
- Automatic screen saver activation after 2 minutes inactivity
- Automatic hibernation activation after 10 minutes inactivity
- Automatics save and shut down after 30 minutes inactivity

Evaluation
This policy will be reviewed bi-annually

Adoption Date: 20 June 2012
Review Date: 01/06/2014
Version Control: V1-18/08/11 V2-01/06/12