IT10
CATEGORY: INFORMATION TECHNOLOGY

CLEAN DESK POLICY

I. PURPOSE

A. Establish the minimum requirements for maintaining a "clean desk" – where sensitive information about employees, Central Coast Community Energy (CCCE) intellectual property, customers and vendors is secure in locked areas and out of sight.

B. A Clean Desk policy is not only ISO 27001/17799 Information Security Management compliant, but it is also part of standard basic privacy control.

II. SCOPE

This policy applies to all CCCE employees and affiliates.

III. POLICY

- Employees are required to ensure all sensitive/confidential information in hardcopy or electronic format is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstation screens must be locked when workspace is unoccupied.
- Any restricted or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing restricted or sensitive information must be kept closed and locked when in use or when not attended.
- Keys used for access to restricted or sensitive information must not be left at an unattended desk.
- Portable computing devices (including laptops and tablets) must be either locked with a locking cable or locked away in a drawer when away from office for a period.
- Passwords may not be left written down in an accessible location.
- Printouts containing restricted or sensitive information should be immediately removed from the printer.
- Upon disposal, restricted or sensitive documents should be placed in the official shredder bin.
- Whiteboards containing restricted and/or sensitive information should be erased.

- Mass storage devices such as USB drives should be treated as sensitive information and be secured in a locked drawer.
- All printouts should be picked up as soon as they are printed; this helps ensure sensitive documents are not left in printer trays for the wrong person to pick up.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

IT staff 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.