IT6
CATEGORY: INFORMATION TECHNOLOGY

IT ACCESS CONTROL POLICY

I. PURPOSE

Prevent unauthorized access to or use of Central Coast Community Energy (CCCE) information, to ensure its security, integrity, and availability to appropriate parties.

II. SCOPE

This applies to all CCCE information and to all storage and access methods.

III. DEFINITIONS

"**Access Control**" refers to enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access (or, providing access to authorized users while denying access to unauthorized users).

IV. POLICY

A. BUSINESS REQUIREMENTS FOR REGULATING ACCESS

Every Information Technology (IT) user shall have a unique identifier and a system password assigned.

There shall be a system in place for authenticating and authorizing users beyond the login point. Access to applications, databases, etc., once a person is in the system must be controlled.

Each user shall be given access to IT resources based on position and tasks performed.

User activity shall be monitored frequently and reviewed for unusual, unauthorized, or illegal activity, current periods of inactivity, etc. User access may be suspended for, but not to limited to, the following:

- A number of consecutive failed log-on attempts;
- Unauthorized or illegal activity; or
- An extended period of account inactivity.

B. MANAGEMENT OF USER ACCESS

Users shall be formally registered at the time of their employment with CCCE. Users shall be re-registered upon changing jobs within CCCE and deleted/un-registered upon leaving CCCE.

Access to CCCE information shall be granted on a need-to-know basis. Users shall be authorized according to their duties. Access may be "read only", "read/write", or "full access" and users may or may not be given administrative privileges for their computers and for certain data.

Additional access may be requested and will be addressed based on a two-step verification process. IT personnel will obtain authorization from both the manager of the department holding the requested data and the CFTO. A supporting reason along with a specific business need will be required before authorization for access is given.

Password Control – refer to Login and Password Security Policy for details.

IT staff shall review all users' access rights/privileges on a regular basis.

C. USER RESPONSIBILITIES

- Users must secure their equipment if it is to be unattended for any length of time. Screen locks should automatically activate after 10 minutes of inactivity (users may set screen locks to activate sooner and they should be allowed to activate screen locks immediately, if desired).
- Users shall have direct access only to services and information that they have been specifically authorized to use. IT staff shall maintain an access control database for tracking of secured data storage locations.

D. OPERATING SYSTEM ACCESS CONTROL

- Access to a local operating system shall be limited to authorized users
- Access to remote operating systems shall be limited to authorized users (for example, IT staff).
- Only authorized support personnel shall be authorized to access remote operating systems and utilities outside of normal business hours.
- Access to remote and local operating systems and related utilities shall be logged and such logs shall be reviewed periodically by IT staff.
- Remote Operating systems connections shall be terminated after 15 minutes of inactivity.

E. MONITORING SYSTEM ACCESS USE

- Instances of access and use of any IT resource shall be automatically logged.
- Access control logs shall be retained in accordance with legal and regulatory requirements.

V. 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.