IT1
CATEGORY: INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY SECURITY POLICY

I. PURPOSE

Outline the conservative approach to securing our information technology (IT) systems and services at Central Coast Community Energy (CCCE) along with the responsibility of staff to enforce this approach. Inappropriate use exposes CCCE to risks including malware, compromise of network systems and services, and legal issues. This policy has been put into place to protect users and CCCE.

II. SCOPE

All users of CCCE's IT systems and services.

III. POLICY

RISK EXPOSURE AND CONTROLS:

CCCE is dependent on IT to conduct its business operations. All CCCE staff are responsible for reporting to management any non-compliance of IT policies. CCCE will make IT accessible only to authorized employees or designated vendors as needed and such information shall only be used for authorized agency purposes. To ensure protection of IT, operational guidelines will be put in place for employees and designated vendors which adhere to the principles below:

1. Access to specific IT is to be assigned to CCCE employees or designated vendors with the minimum level of access necessary to perform respective responsibilities.
2. Access to IT will be made available only to the extent necessary to support authorized business functions.
3. Security systems will be structured with multiple layers of security, including physical, network, host, and personnel security measures.
4. The degree of information security protection is to be commensurate with the impact of inadvertent or intentional misuse, improper disclosure, damage, or loss.
5. Adequate controls will divide sensitive duties among more than one individual to provide checks and balances that help ensure operational guidelines are followed.
6. Security is not an optional component of operations. All CCCE staff and designated vendors are required to protect information. All staff and designated vendors that use or have access to CCCE IT are personally responsible for exercising the proper control over information according to the operational guidelines provided to them.

7. Operational guidelines for treatment of IT are subject to change as needed to protect CCCE and its customers based on any changes in systems, threats, and practices.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

IT staff will verify compliance to IT 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 IT policy may be subject to disciplinary action, up to and including termination of employment.