IT5
CATEGORY: INFORMATION TECHNOLOGY

INTERNET USAGE POLICY

I. PURPOSE

Provide Central Coast Community Energy (CCCE) staff with rules and guidelines about the appropriate use of network and Internet access. Having such a policy in place helps to protect both the business and the employee; the employee will be aware that browsing certain sites or downloading files is prohibited and that the policy must be adhered to, thus leading to fewer security risks for the business as a result of employee negligence.

II. SCOPE

All users of CCCE's network/internet infrastructure.

III. DEFINITIONS

"**Information Systems**" refers to all resources that store, transmit or present information related to CCCE business

"**Resources**" refers to all CCCE-owned hardware and software including, but not limited to:

- Computers, laptops, tablets, phones
- Monitors, printers, scanners,
- Network storage, network infrastructure, servers
- All software applications licensed by CCCE
- Accounts such as email account or other accounts used to access CCCE applications
- Data plans, subscription services
- Audio and video equipment

IV. POLICY

A. ACCEPTABLE USE

- This Internet Usage Policy applies to all employees of CCCE who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees of CCCE is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through CCCE is a privilege and all employees must adhere to the policies concerning Computer, Email and Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations of this policy.
- Company employees are expected to use the Internet responsibly and productively.
- All Internet data that is composed, transmitted and/or received by CCCE computer systems belongs to CCCE and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services, and technology used to access the Internet are the property of CCCE and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.
- All sites and downloads may be monitored and/or blocked by CCCE if they are deemed to be harmful and/or not productive to business.

B. STRICTLY PROHIBITED USE

- Sending or publishing discriminatory, harassing, or threatening messages or images
- Using an unauthorized VPN or other encryption/usage masking service
- Using computers to perpetrate any form of fraud or digital piracy
- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying, or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside CCCE
- Hacking into unauthorized websites
- Sending or posting information that is defamatory to CCCE, its products/services, colleagues and/or customers
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems.

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.