IT2
CATEGORY: INFORMATION TECHNOLOGY

INFORMATION SYSTEM AND SERVICE USE POLICY

I. PURPOSE

Outline the acceptable use of Central Coast Community Energy (CCCE) information technology (IT) systems and services. Inappropriate use exposes CCCE to risks including malware, compromise of network systems and services, and legal issues. Therefore, this policy has been put into place to protect users and CCCE.

II. SCOPE

All users of CCCE's IT systems and services.

III. DEFINITIONS

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

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

"**Information Technology (IT) Systems and Services**" refers to all resources that store, transmit, or present information related to CCCE business.
Examples: Laptop, Local Area Network (LAN), or cloud services like DocuSign

"**Data**" is all information stored or transmitted over CCCE information systems or services.

"**Sensitive Information**" includes all data, in its original and duplicate forms, which contains personal information, protected health information, customer record information, card holder data, confidential personal data, or information that is deemed to be confidential or is otherwise exempt from disclosure under state law.

"**User**" is anyone using CCCE IT systems or services including, but not limited to: employees, contractors, limited-term employees, and interns.

IV. POLICY

A. ACCEPTABLE USE

Use of CCCE's IT systems and services is limited to CCCE business.

Access, use, or share CCCE proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

All users are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor.

B. STRICTLY PROHIBITED USE

Use of CCCE IT systems or services to send messages of a threatening, harassing, or obscene nature, or any behavior found to be inconsistent with the CCCE Employee Handbook, is prohibited. Inappropriate use may include, but is not limited to:

- The display or transmission of sexually explicit images, messages, or cartoons.
- Any transmission that contains ethnic slurs, racial epithets, or anything that constitutes harassment or disparagement of others based on their race, national origin, color, sex, sexual orientation, age, disability, religious, or political beliefs.

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CCCE.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CCCE or the end user does not have an active license is strictly prohibited.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

C. SECURITY AND PERSONAL INFORMATION

All IT systems and services are to be secured with credentials meeting the CCCE Login and Password Security Policy. Users who are granted access to any part of CCCE's IT systems or services are provisioned with an account.

Users are to use their assigned account and no other. Users are prohibited from using another user's account to access any part of an IT system or service.

Users are prohibited from sharing their passwords or passphrases. Authorized staff may reset passwords as required for business purposes. Users who are provisioned with CCCE resources are not allowed to change permissions, modify hardware, or modify code and configuration on any CCCE resource, unless directed to do so by authorized personnel.

All users are responsible for safeguarding sensitive information. Users may access, use, or share sensitive information held by CCCE only to the extent it is authorized and necessary to fulfill their assigned job duties. Users must immediately notify IT staff if sensitive information is inappropriately shared or exposed.

D. NO EXPECTATION OF PRIVACY

CCCE owns all data stored on CCCE resources and reserves the right to access anything the user has viewed or created using those resources.

Users shall have no expectation of privacy. Authorized CCCE staff may view all activities and data created, stored, or transmitted using CCCE resources. They may access any electronic data at any time without consent from or notification to the user.

CCCE may monitor, record, or review any data or websites a user may have accessed through an CCCE internet connection.

CCCE strongly discourages the storage of personal files and messages (pictures, personal email, texts, instant messages, music, spreadsheets, etc.) on CCCE resources. All such data may be accessed and reviewed at the CCCE's discretion and may be deleted without notice.

E. HARDWARE AND SOFTWARE CONTROL

- Alteration, upgrade, or modification to IT resources such as computer equipment, software, services, or IT infrastructure is prohibited without IT approval.
- No software installation is allowed by a user without IT staff approval.
- User is not allowed to attach any non-company issued or unauthorized device, such as a USB storage device, printer, or video cam, to the company's computer equipment, network equipment, or other IT resource. This restriction includes the unauthorized installation of any additional network-related or digital communications equipment such as routers, network switches, or wireless access points.
- CCCE retains ownership of all company-owned hardware, software programs, and service subscriptions provided to users. CCCE is not responsible for any computer equipment that is not provided by CCCE.
- User is responsible for taking all reasonable safety precautions with mobile devices (laptops and mobile phones) to protect them from theft or physical damage.
- User must report to his/her supervisor and IT staff, as soon as possible, in the event of any computer equipment loss.

F. RESTITUTION

Should a user fail to return CCCE-provided computer equipment upon termination, the company reserves the right to ask the user to pay the current market value of the equipment as determined by the CEO.

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.