IT13
CATEGORY: INFORMATION TECHNOLOGY

INFRASTRUCTURE FAILURE RESPONSE

I. PURPOSE

Establish the response to any situation severely impacting Central Coast Community Energy (CCCE) business continuity. This policy will clearly define staff roles and responsibilities, to whom it applies and under what circumstances, standards, and metrics (e.g., to enable prioritization of the incidents), as well as reporting and remediation mechanisms. The policy shall be well publicized and made easily available to all personnel involved in the recovery process.

II. SCOPE

This policy applies to any situation in which the information technology infrastructure is compromised or otherwise rendered inoperable to the extent business is unable to be conducted.

III. DEFINITIONS

"**Information Technology (IT) Asset**" refers to any computer hardware, network hardware, software, service, or Information Technology-based CCCE information. In this context, "asset" and "Information Technology (IT) Asset" are understood to be the same.

"**Information Technology (IT) Service**" refers to any data or voice connection, file share, data store, email, communication medium. In this context, "service" and "Information Technology (IT) Service" are understood to be the same.

IV. POLICY

When an occurrence takes place that impacts the IT infrastructure, the IT staff will be contacted at the earliest opportunity. After the IT staff have assessed the situation, the CFTO will be updated along with the CEO.

The CEO will chair an incident response team to handle the incident. The team will include (based on availability) members from:

- Finance and Technology
- Affected unit(s) or department(s)
- Additional individuals as deemed necessary by the CEO

IT staff, along with the designated team, will analyze the situation to determine the effected assets and services. After the effected assets and services have been identified, IT personnel along with the CFTO will determine the most expedient and cost-effective means of replacing the needed assets and services by reaching out to standard vendors. Every effort will be made to put in place temporary solutions to address immediate needs such as internet and phone connections along with data access requirements.

The majority of CCCE data is currently stored in the cloud on a secure platform. The data is accessible via secure sign-in and can be made available at any time. Should data stored on the cloud service become corrupted or otherwise made unusable, a dedicated cloud backup is in place to allow for the restoration of data.

The business data currently stored on local devices such as Network Attached Storage (NAS) or local server, serves as backup to cloud storage and can be used to restore some online services/data.

Email is currently hosted in the cloud on a secure platform. Email is accessible via secure sign-in and can be made available at any time. Should data stored on the cloud service become corrupted or otherwise made unusable, a dedicated cloud backup is in place to allow for the restoration of data.

Servers hosted in the cloud on a secure platform, are backed up on a regular basis and restoration is available on demand.

The incident response team will communicate the decided response plan to the staff along with an estimated timeline of IT asset and service replacement and availability.

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.