IT8
CATEGORY: INFORMATION TECHNOLOGY

DATA BREACH RESPONSE POLICY

I. PURPOSE

Establish the response to a Central Coast Community Energy (CCCE) data breach. This policy will clearly define Data Breach, to whom it applies and under what circumstances, staff roles and responsibilities, standards, and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

CCCE Information Technology's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how CCCE's established culture of openness, trust, and integrity should respond to such activity. CCCE Information Technology is committed to protecting CCCE's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

II. SCOPE

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of CCCE customers, employees, and protected information of suppliers.

III. DEFINITIONS

"**Encryption or encrypted data**" – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.

"**Plain text**" – Unencrypted data.

"**Hacker**" – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

"**Protected Health Information (PHI)**" - Any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

"**Personally Identifiable Information (PII)**" - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data.

"**Protected data**" - See PII and PHI.

"**Information Resource**" - The data and information assets of an organization, department or unit.

"**Safeguards**" - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

"**Sensitive data**" - Data that is encrypted or in plain text and contains PII or PHI data (see PII and PHI above).

IV. POLICY

A. GENERAL

As soon as a theft, data breach or exposure containing CCCE's Protected data or CCCE's Sensitive data is identified, the process of removing all access to that resource will begin.

The CEO will be notified of the theft, breach or exposure and IT personnel will immediately change all passwords on the effected platform (e.g. Firewall, Email Infrastructure, File Shares, etc.).

The CEO will chair an incident response team to handle the breach or exposure. The team will include members from:

- Internal Operations;
- IT Supports;
- Communications and External Affairs;
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed;
- Additional departments based on the data type involved;
- Additional individuals as deemed necessary by the CEO.

IT Support, along with the designated team, will analyze the breach or exposure to determine the root cause. After the cause is determined IT personnel will take appropriate security measures to mitigate a future occurrence.

B. DEVELOP A COMMUNICATION PLAN

The incident response team will decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

IV. 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.