Central Coast Community Energy

CLEAN ENERGY. LOCAL CONTROL.
3CEnergy.org

IT11
CATEGORY: INFORMATION TECHNOLOGY

THREAT RISK ASSESSMENT

I. PURPOSE

Central Coast Community Energy (CCCE) shall regularly evaluate its Information Technology (IT) systems and services for threats and vulnerabilities to protect its IT and reduce the risk to CCCE.

II. SCOPE

This procedure applies to all CCCE's IT systems and services.

III. DEFINITIONS

"**Risk**" is the possibility of losing availability, integrity, or confidentiality of IT assets due to a specific threat; also, the product of threat level and vulnerability level.

"**Threat**" is an expression of intent to inflict injury, damage, or security violation.

"**Threat Assessment**" is a process by which types of threats an IT network might be vulnerable to and where the network is most vulnerable are identified.

”**Vulnerability**" is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited.

IV. POLICY

A. IT THREAT & RISK ASSESSMENT – INTRODUCTION

To prepare for threats to its IT assets and infrastructure, CCCE must be aware of the types of threats that exist, the likelihood that they will occur, their potential impact, and the risk these threats may pose.

Threats may be natural or manmade. Natural threats include floods, storms, and earthquakes. Manmade threats may be accidental or intentional. Examples of manmade threats include use of unauthorized hardware or software and having unauthorized access to CCCE systems. Intentional threats exist both outside CCCE and within.

The risk posed by any given threat is a function of the combined likelihood of the threat occurring and the impact it would have on CCCE's assets (hardware, software, data, network/infrastructure, and personnel) if it were to occur. While risk to CCCE's IT assets cannot be eliminated, CCCE must make all reasonable efforts to minimize risk. Those efforts should begin with assessing threats and risks.

B. IT THREAT ASSESSMENT PREPARATION

In advance of conducting a Threat Assessment of any of CCCE's IT systems, IT staff shall establish a baseline for assessment, identifying systems to be assessed (data storage, IT systems, IT services, etc.) and determining their interconnectivity with other systems.

IT staff should identify and describe threats that may target the IT assets and systems under consideration by one or more of the following means:

- Periodically reviewing Access Control Log for threat occurrences, such as unauthorized system access.
- Reviewing IT incidents for trends and/or patterns.
- Reviewing any system test (test script, test procedures, expected results, etc.) for vulnerabilities testing.
- Conducting penetration testing at irregular intervals, to verify the IT network's ability to withstand intentional attempts at circumventing IT security.

IT staff may acquire additional information for developing the assessment baseline by routinely reviewing alerts and bulletins from vendors, standards organizations, etc.

To determine if CCCE needs to act on any given threat and to what extent it should act, IT staff shall classify the likelihood of threats/vulnerabilities in the following manner:

- **Low** – the threat is unlikely to occur;
- **Medium** – the threat may occur. For example, CCCE is located in an earthquake zone, so an earthquake is likely to have an effect on CCCE;
- **High** – the threat is likely to occur. For example, if CCCE does not require password access to computers or data stores, the likelihood is high that someone will eventually access and steal or compromise CCCE data.

To determine if CCCE needs to act on any given threat and to what extent it should act, IT staff shall classify the impact of threats/vulnerabilities in the following manner:

- **Low** – the threat may result in minimal loss of CCCE assets/resources;
- **Medium** – the threat may result in a significant loss of CCCE assets/ resources, harm CCCE's mission or interests, or result in injury to an employee;
- **High** – the Threat may result in a very costly loss of CCCE's assets/resources, significantly harm CCCE's mission, interests, or standing, or result in serious or fatal injury to an employee.

An exposure rating or Risk assessment shall be based on likelihood and impact ratings. A Risk matrix is prescribed (Figure 1), with likelihood running from low to high along one axis and impact running from low to high on the other axis.

FIGURE 1 – RISK MATRIX

	Impact	Low	Medium	High
Likelihood	High	Low	Medium	High
	Medium	Low	Medium	Medium
	Low	Low	Low	Low

The exposure rating/risk assessment shall be used to prioritize threats (Figure 2).

- **High**-risk threats require the highest security levels and present the greatest need for immediate action if existing security tools and techniques are inadequate.
- **Medium**-risk threats require a response to be scheduled for implementation within a reasonable timeframe.
- **Low**-risk threats may require little or no response on the part of the IT staff.

FIGURE 2 – THREAT PRIORITY

Risk Level	Description and Actions
High	Preventive actions are required and a preventive action plan shall be developed and implemented as soon as possible.
Medium	Preventive actions are required and a plan to incorporate those actions within a reasonable time frame shall be developed.
Low	IT Support should confer with managers of affected systems to determine if preventive action is required or if risk is acceptable.

C. IT THREAT/RISK ASSESSMENT

At regular intervals, IT staff shall conduct a threat/vulnerability assessment of the IT network. IT staff shall review the results and analyze the findings in order to determine if action is required and to what extent.

D. IT THREAT/RISK REVIEW

IT staff shall periodically review the risk assessment process to ensure its continued timeliness and applicability. Historical data (i.e., number, nature, and severity of threats over time) shall help determine if risks are under control.

Any time a significant implementation, revision, etc., takes place, IT staff shall review the risk assessment process, to ensure existing controls are applicable to such changes or if improved controls are required. This may include updating IT Policies for approval.

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.