PENINSULA CLEAN ENERGY

Policy Number: 20.c
Board Adoption: December 20, 2018

Information Technology Security Policy

Overview and Purpose

The purpose of this policy is to ensure proper management of information technology (IT or Information) as required to support regulatory compliance, minimize legal liability, reduce the risk of criminal activity, and sustain stakeholder and customer satisfaction. The IT of Peninsula Clean Energy (PCE) is a critical asset that will be managed to ensure that it remains complete, accurate, confidential, and available for authorized business activities.

1. **Data protection requirements**

   Data is a valuable asset of PCE, and some data must be protected with a higher level of attention and caution. The level of protection is based on the method defined after evaluating the type and sensitivity of the data in question.

2. **Information Access and Controls**

   PCE will make information technology accessible only to authorized employees or designated vendors as needed and such information shall only be used for authorized PCE purposes. To ensure protection of information technology, operational guidelines will be in place for employees and designated vendors to follow which adhere to the principles below:

   a. Access to specific information technology is to be assigned to PCE employees or designated vendors with the minimum level of access necessary to perform respective responsibilities.
   b. Access to information technology will be made available only to the extent necessary to support authorized business functions.
   c. Security systems are to be structured with multiple layers of security, including physical, network, host, and personnel security measures.
   d. The degree of information security protection is to be commensurate with the impact of inadvertent or intentional misuse, improper disclosure, damage or loss.
   e. Adequate controls will ensure effective segregation of duties to provide checks and balances that help insure operational guidelines are followed. Some of the key operational practices PCE follows include; system encryption, using only the authorized cloud management platform to store documents, and setting-up two factor authentication.
   f. Security is not an optional component of operations. All PCE staff and designated vendors are required to protect information. All staff and designated vendors that use or have access to PCE information technology are personally

responsible for exercising the proper control over information according to the operational guidelines provided to them.

g. Operational guidelines for treatment of information technology are subject to change as needed to protect PCE based on any changes in systems, threats, and practices.
h. PCE will retain customer energy usage data only for as long as reasonably necessary or as authorized by the California Public Utilities Commission to accomplish a specific authorized purpose**.**

3. **Specific roles and responsibilities**

a. **Finance Department**: PCE's Finance Department is responsible to define and implement key IT policies, ensure compliance with the policies, and perform periodic assessment to make sure policies are updated as needed.

b. **Data user**: The data user is the individual, automated application or process that is authorized to create, enter, edit, and access data, in accordance with the policies and procedures. Data users have a responsibility to:

i. Maintain the security of passwords, personal identification numbers (PINs), and authentication tokens and certificates, and will be held accountable for any activities linked to their accounts;
ii. Use the data only for the purpose specified by the Finance Department;
iii. Comply with controls established by the Finance Department;
iv. Prevent disclosure of confidential or sensitive data; and
v. Report suspected security incidents that may have breached the confidentiality of data.

c. **Individuals using personally owned computers and other network devices**: Staff and consultants should use personally owned systems or devices only when absolutely necessary. Staff and consultants who use personally owned systems or devices to access PCE resources are responsible for the security of those systems and devices and are subject to:

i. The provisions of this IT Security Policy and the standards, procedures, and guidelines established by the Finance Department for PCE computing and network facilities, and
ii. All other laws, regulations, or policies directed at the individual user.

d. **Third-party vendors**: Third-party vendors providing hosted services and vendors providing support, whether on site or from a remote location, are subject to PCE security policies and may be required to acknowledge this fact in the contractual agreements.

e. **Other registered entities**: Any entity that is a registered user and connected to PCE's network is responsible for the security of its computers and network devices and is subject to the following:

    i. The provisions of this IT Security Policy and the standards, procedures, and guidelines established by the Finance Department for PCE computing and network facilities.
    ii. All other laws, regulations, or policies directed at the organization and its individual users.

4. **Reporting of security incidents**

A critical component of security is to address security breaches promptly and with the appropriate level of action. All individuals are responsible for reporting incidents in which they suspect data, computer or network security may have been compromised. All such suspected or actual incidents should be reported to the Finance Department.