PENINSULA CLEAN ENERGY

Policy Number: 8
Board Adoption: October 27, 2016

Information Technology and Security

Overview and Purpose

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

1. Risk Exposure and Controls

PCE is dependent on information technology to conduct business operations. PCE's CEO, in collaboration with the IT Consultant, are developing company IT policies and standards, identifying areas of risk, and helping all personnel achieve compliance with policies and standards. All PCE staff are responsible for reporting to management on any non-compliance. PCE will make information technology accessible only to authorized employees or designated vendors as needed and such information shall only be used for authorized agency 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 divide sensitive duties among more than one individual to provide checks and balances that help insure operational guidelines are followed.

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.