Customer Service Policy A.4
Information Technology (IT) Security Policy

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

SCPA is dependent on information technology to conduct business operations. The Chief Executive Officer, Chief Operating Officer, Director of Internal Operations, and Director of Customer Service, in collaboration with SCPA's IT Consultant have been designated as the IT Security Team (IST) and are responsible for communicating IT policies and standards, helping all personnel achieve compliance with policies and standards, and reporting to management on any non-compliance or areas of risk.

SCPA 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:

- Follow all SCPA Board of Directors polices.
- Access to specific information technology is to be assigned to SCPA employees or designated vendors with the minimum level of access necessary to perform respective responsibilities.
- Access to information technology will be made available only to the extent necessary to support authorized business functions.
- Security systems are to be structured with multiple layers of security, including physical, network, host, and personnel security measures.
- The degree of information security protection is to be commensurate with the impact of inadvertent or intentional misuse, improper disclosure, damage or loss.
- Adequate controls will divide sensitive duties among more than one individual to provide checks and balances that help ensure operational guidelines are followed.
- Security is not an optional component of operations. All SCPA staff and designated vendors are required to protect information. All staff and designated vendors that use or have access to SCPA information technology are personally responsible for exercising the proper control over information according to the operational guidelines provided to them.

Operational guidelines for treatment of information technology are subject to change as needed to protect SCPA based on any changes in systems, threats, and practices. All substantive changes will be brought back before SCPA's Board of Directors for formal approval.

Adopted: February 7, 2019
Amended: October 1, 2020