DCE POLICY # 18-07
Information Technology Security

Subject: Policy governing information technology and data controls

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

Risk Exposure and Controls: DCE is dependent on information technology to conduct its business operations. All DCE staff are responsible for reporting to management any non-compliance of this policy. DCE will make information technology accessible only to authorized employees or authorized/designated vendors as needed, and such information shall only be used for authorized agency purposes. To ensure protection of information technology and adherence to protocols, operational guidelines will be put in place for employees and designated vendors which will adhere to the principles below:

• Access to specific information technology is to be assigned to designated DCE employees or 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 will 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 insure operational guidelines are followed.

• Security is not an optional component of operations. All DCE staff and designated vendors are required to protect sensitive data and customer information. All staff and designated vendors that use or have access to DCE information technology are personally responsible for exercising the proper control over information assets according to the operational guidelines provided to them.

• Operational guidelines for treatment of information technology are subject to change as needed to protect DCE and its customers based on any changes in systems, threats, and practices.