Sunnyslope County Water District
Computer Security & Information Technology Policy

8000: Computer Security & Information Technology

8000.1 Purpose.

Sunnyslope County Water District seeks to ensure that detailed or sensitive information regarding its water and wastewater system facilities and operations not be released to parties who might use it for malicious purposes. This security policy is designed to address computer security procedures for District personnel who are issued desktop and/or laptop computers and who may handle sensitive or important information to the operation of the District. This information technology policy is also designed to address how changes to the computer system, applications, databases, and operating systems will be approved and documented.

8000.2 Scope.

This policy applies to all employees who are issued desktop or laptop computers and who have oversight of District computer based applications, databases, and operating systems.

8000.3 Responsibilities.

A. The Finance Manager, approves all purchases of desktop or laptop computers for use by District personnel, subject to the General Manager's oversight.

B. Department managers are responsible for assigning laptop computers to personnel within their respective departments, and for enforcement of this policy.

C. Each employee issued a desktop or laptop computer is responsible for understanding and following the requirements of this policy.

D. The General Manager may designate a Network Administrator to oversee and manage the network and adherence to this policy.

8000.4 Sensitive Information.

Sensitive information that must not be released has been classified by the Federal Energy Regulatory Commission as Critical Energy Infrastructure Information and includes electrical, civil, and mechanical schematics and drawings that show details of location and layout. The District also considers detailed maintenance records that include photos and schedules to be sensitive information. No District documents may be downloaded to a portable drive and removed from the District property without prior approval of the General Manager or Network Administrator.

8000.5 Computer Security.

A. Passwords. A password will be required to start the desktop or laptop computer. Passwords must be a minimum of six (6) characters in length and must contain at least

one (1) number and one (1) special character.

1. Passwords are confidential and unique, and should NOT be written down, except however, a written documentation of desktop/laptop and software application passwords may be kept in the employees' personnel file.

2. Passwords are to be changed at least annually.

3. The General Manager and the designated Network Administrator manage network access.

B. Anti-Virus Protection. All desktop and laptop computers will have anti-virus software installed and should be set to run and update automatically. No documents or files can be uploaded from a portable drive without first obtaining authorization from the General Manager and/or Network Administrator and scanning with anti-virus software.

C. Any software installed on the desktop or laptop computer must be pre-approved by the Network Administrator.

D. Internet access may only be made through the District's network server. The desktop or laptop computer may not be used to access the Internet via an employee's personal Internet account.

E. The portable laptop computer may be transported between the main District office and the field location at which the employee is assigned to work via a District vehicle. If the employee at any time leaves the vehicle unattended, the laptop computer will be stored out of sight in a locked compartment.

F. All electrical, civil, and/or mechanical schematics, drawings, photos, and database records will be stored in electronic format on the District's network computer. Only those schematics, drawings, photos, or maintenance database records necessary for the work being conducted at the given field location may be downloaded and temporarily stored on the laptop computer's hard drive. Upon completion of the field assignment, all revised files will be uploaded onto the District's network computer and all temporarily stored files will be deleted from the laptop computer's hard drive.

G. Any desktop or laptop computer may not be removed from the District's service area without prior approval of the General Manager and/or the Network Administrator.

8000.6 Network Security.

District networks with access to the Internet must be protected by a firewall approved by the Network Administrator. Employees must abide by departmental, local, state, federal, and Internet Service Provider (ISP) security policies as they apply to use within the District. The District routinely monitors usage patterns for its network communications for purposes of cost

analysis, allocation, and managing the District's gateway to the Internet. All those using public networks such as Internet, Intranet, and electronic mail should be aware that any messages created, sent, or retrieved over the District's network are not private. Employees should use discretion when using public networks (e.g. Wi-Fi hotspots) with non-encrypted data if data security and confidentiality is an issue. Access to system and network operating manuals is restricted and managed by the General Manager and the Network Administrator.

A. **Modems.** The Network Administrator approves, manages, audits, and inventories all dial-out or dial-in modems connected to the local area network. Modems must meet all security requirements for the local network and must not pose a threat to wide area network security.

B. **Physical Environment.** The proper physical environment will be maintained for workstations, servers, and network hardware. Manufacturer specifications dictate temperature and humidity limits. Servers and network equipment require secure/locked environments for security purposes. All servers and critical network components need back-up power supplies in case the primary power fails.

C. **Network Device Installations.** The Network Administrator must be notified before attaching any new devices that could affect the wide area network or other local area networks.

D. **Backups.** All documents created on any desktop or laptop are to be saved to a network drive to ensure they are backed up.

1. **Network Server.** The network is scheduled to run backups automatically. The two backup drives, Server 1 and Server 2, are rotated on a daily basis Monday through Friday and logged on the backup tracking sheet. The backup drives are stored in the Safe.

2. **Utility Billing/Customer Accounts (Mom's).** A backup is done daily, except weekends and at certain points during the monthly billing cycle per the written billing procedures. Backups are stored in the safe, except a month-end backup is created each month and is stored off-site with the General Manager.

3. **General Ledger (QuickBooks).** A backup is done every Friday, at the end of the day and stored in the Safe for a minimum of three months.

8000.7 Modifications to Computer Systems, Applications, Databases, and Operating Systems.

Any modifications, changes, or non-routine upgrades to the computer systems, applications, databases, and operating systems must be approved by the General Manager before implementation.

8000.8 Compliance.

The General Manager or Network Administrator will periodically check all desktop or laptop computers to ensure that no critical infrastructure information or other sensitive data is being stored on the computer's hard drive. Personnel found to be in violation of this policy will be subject to disciplinary procedures.

Policy Approved: March 12, 2014
Date