

Sacramento Suburban Water District

Information Technology/Disaster Recovery Policy

Adopted: April 21, 2008
Revised: February 22, 2010

100.00 Purpose of the Policy

The purpose of this policy is to establish and ensure appropriate guidance and acceptable usage, responsibilities, security, and protection of District electronic facilities (DEF), e.g., computers, laptops, servers, telephones, voice mail, fax machines, software, cell phones, smart phones, internet, email, personal digital assistants (PDAs), printers, and copiers.

Resource constraints dictate that the District will facilitate its support effectiveness of DEF through such means as the following:

1. Maximizing system uniformity with standard configurations.
2. Sustaining the DEF program by periodically upgrading and replacing DEF on a regular cycle.
3. Ensuring that DEF and their support resources are allocated to meet the needs of the District's Strategic Plan.

100.10 District Property

All DEF are the sole property of the District. All messages sent and received, including any personal messages, and all data and information stored on DEF are the District's property regardless of content.

All software acquired for or on behalf of the District or developed by District employees or contract personnel on behalf of the District is and shall be deemed District property.

100.20 Disaster Recovery

In the event of a critical disaster to DEF at one of the District's primary facility locations (Marconi or Walnut office), the District will have in place the necessary DEF at both facility locations such that critical functions can be operational as soon as possible. For critical disasters at both District primary facilities simultaneously, the District will keep an off-site backup system of District data such that recovery can occur as expeditiously as possible.

100.30 Authorized Usage

Only authorized District staff or contract personnel are to use DEF. All electronic communications using DEF are to be used solely for District-related business purposes and not for personal use.

100.40 Unauthorized Usage

Unless pre-approved by the Information Technology (IT) Manager or the General Manager personal software and equipment connected to the DEF is not authorized, including, but not limited to:

1. A piece of software purchased for one's home computer
2. A downloaded title from the internet
3. Any proprietary title not licensed to the District

(See "Employee Policy and Procedures Manual" Section 7.5 "E-Mail/Internet/Computer Use.")

200.00 Technology Procurement

All District hardware and software purchased shall be coordinated with the IT department to ensure that all applications conform to District standards and are purchased at the best possible price.

300.00 Information Security

It is the responsibility of each employee to protect data belonging to the District. The following guidelines are for all employees:

- All DEF must be monitored and secured at all times by District staff.
- Any loss, theft, or suspicious activity of DEF must be reported to the IT Manager immediately.
- For security and network maintenance purposes, authorized individuals with District approval may monitor equipment, systems and network traffic at any time.

400.00 Policy Review

This Policy shall be reviewed at least biennially.