Sacramento Suburban Water District

Technology Maintenance, Security, Protection and Recovery Policy

Adopted: April 21, 2008
Approved with Changes: September 19, 2022

100.00 Purpose of the Policy

The purpose of this policy is to establish and ensure appropriate guidance for the maintenance, security, protection, and recovery of District electronic facilities including computers, servers, printers, scanners, software, Internet, Intranet, phones, copier/fax machines and all other technology-related devices and data.

100.10 General

The District's goal is to conform to the "Best Practices" as contained in the "15 Cybersecurity Fundamentals for Water and Wastewater Utilities" as published by the Water Information Sharing and Analysis Center (WaterISAC). This policy contains several of the Best Practices recommended by WaterISAC. Additional Best Practices are contained in other various District Policies and Procedures. (WaterISAC #9)

200.00 Electronic Facilities Maintenance and Support

Prudent management practices dictate that the District will facilitate its maintenance and support of District electronic facilities through such means as the following:

1. Maintaining an electronic facilities inventory. (WaterISAC #1)
2. Investing in both staff and technology resources to ensure adequate support and maintenance of all District electronic facilities.
3. Maximizing system uniformity with standard configurations.
4. Sustaining District electronic facilities by periodic upgrades and replacements on a regular cycle.
5. Ensuring that District electronic facilities and their support resources are allocated to meet the needs of the District's strategic plans.

200.10 District Property

All District electronic facilities are the sole property of the District. All messages sent and received, including any personal messages, and all data and information stored on District electronic facilities 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.

200.20 Authorized Usage

Only authorized District staff or contract personnel, pre-approved by the General Manager (GM) or the Information Technology Manager (IT Manager), are to use District electronic facilities. All usage of District electronic facilities is to be conducted solely in accordance with the District's Technology Use Policy (PL – IT 005). (WaterISAC #13)

200.30 Technology Procurement

All District hardware and software purchased or developed shall be coordinated with the IT Department to ensure that all hardware and software conform to District standards, are compatible with District systems, and are purchased or developed at the best possible price.

200.40 Electronic Facilities and Data Security

Appropriate hardware and software monitoring shall be in place to ensure the protection of District data as well as all District electronic facilities. Appropriate security measures will include, at a minimum, the following:

1. Maintaining protected backups of District servers and data both on and off-site.
2. Educating District staff on basic security, personal cybersecurity and methods of malicious actors and attacks. Develop a culture of cybersecurity awareness amongst staff. (WaterISAC #8)
3. The use of strong passwords and multi-factor authentication. (WaterISAC #4)
4. Utilization of tools and external resources to monitor, track, report and respond to suspicious activity within District electronic facilities. (WaterISAC #10)
5. Stay aware of current vulnerabilities. Perform timely updates to software and firmware. (WaterISAC #7)
6. Maintain security trained IT staff and/or partnerships with 3rd party security experts.
7. For security and network maintenance purposes, authorized individuals, with IT Manager, Director of Finance and Administration, Assistant General Manager or GM approval, may monitor equipment, systems and network traffic/activity at any time.

It is the responsibility of each employee to protect District electronic facilities and data. All employees, by their use of electronic facilities, are part of the District's cybersecurity program. Each employee plays a vital role in protecting the District from cyberattacks. Cyberattacks include all methods of gaining access to District electronic facilities and data for the purpose of causing damage, harm, extortion or the stealing of District information by means of malware, viruses, hacking, social engineering or actual physical access. The following guidelines are for all employees:

1. All District electronic facilities and data must be secured at all times by District staff and contract personnel. (WaterISAC #5)
2. Any loss, theft, or suspicious activity of District electronic facilities or data must be reported to the IT Department immediately.
3. Employees are to use extreme care when opening links or attachments to ensure

they are free from viruses or malicious code that could infect District electronic facilities and data. Files that are downloaded from the internet or received via electronic communications must be checked with virus detection software before being opened and used.

4. Passwords are to be kept secure and employees should never share passwords with another individual. Passwords should be appropriately complex to eliminate easy guessing or deciphering. Passwords should be periodically changed. (WaterISAC #4)
5. All District employees will participate in cybersecurity awareness training. (WaterISAC #8)

200.50 Disaster Recovery

The District will maintain procedures and plans that will address disaster recovery from various disaster types. The District maintains an Emergency Response Plan which includes particular electronic facilities disaster response scenarios. The District will maintain additional disaster response plans to cover scenarios not part of the Emergency Response Plan. Refer to Procedure PR – IT 003 Technology Maintenance, Security, Protection and Recovery Procedure, section 700, for specific disaster recovery procedures. (WaterISAC #11)

The District will maintain electronic facilities disaster preparedness at all times. The District will regularly test its electronic facilities disaster preparedness. Disaster preparedness will address, at a minimum, the following situations:

1. Electrical outages
2. Loss of communications:
    a. Network communications
    b. Internet communications
    c. Telephony communications
    d. Cellular communications
    e. Radio communications
    f. Satellite communications
3. Data backup and recovery
    a. On premise
    b. Cloud based
4. Cyberattacks and data breaches
5. Virus and malware attacks
6. Data corruption
7. Hardware failures
8. Software and firmware update failures

In the event of a critical disaster to District electronic facilities or data at one of the District's primary facility locations (Marconi or Walnut office), the District will have in place the necessary District electronic facilities 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 of District data such that recovery can occur as expeditiously as possible. The District will maintain partnerships with 3rd party electronic facilities providers to assist in system recovery in the event of a critical disaster at both primary facilities.

Specific steps for how District electronic facilities will be protected and how and when the District's critical systems will be back online will be kept as part of IT Procedure PR – IT 003 and updated as necessary.

300.00 Policy Review

This Policy shall be reviewed by the Board of Directors at least biennially.