DIABLO WATER DISTRICT

REGULATION NO. 126

CYBERSECURITY

Section I. Purpose.

A. The main purpose of the District's Cybersecurity Program is to help prevent, detect, respond to, and recover from cyber security threats.

Section II. Overview.

A. The program outlined in this regulation, and confidential policy/procedure documents (not included for security reasons), were developed and based upon the best practices and guidelines set by the National Institute of Standards and Technology (NIST); Water Information Sharing and Analysis Center (WaterISAC); American Water Works Association (AWWA); and the United States Environmental Protection Agency (EPA). **Diablo Water District intends to follow all applicable cybersecurity recommendations from those agencies.**

B. The underlying theme is modelled after the Department of Homeland Security's, "If You See Something, Say Something" program.

Section III. Cybersecurity Program.

A. Routine Asset Inventories.

1. Maintain log of approved physical electronic devices, cloud systems, data storage, virtual connections, smart devices, etc.

2. If inventory identifies unauthorized asset(s), a threat assessment shall be performed and unauthorized asset removed from the District's network infrastructure.

B. Assess Risks.

1. Perform an internal risk assessment, at a minimum, annually.
2. On a tri-annual basis hire a third party to perform the risk assessment.

C. Minimize Control System Exposure.

1. Eliminate all non-secure communication access paths.
2. Segment networks to limit exposure.
3. Maintain role-based security clearance.
4. Encrypt communication when possible.
5. "Lock down" the network to only be accessed by approved devices.

D. Enforce User Access Controls.

1. Use role-based access control to limit the ability of individual users.
2. Use the principle of limiting the access to network information to the minimum required for the specific users to perform their job.
3. Ensure default passwords are not used.
4. Implement multi-factor authentication where possible.
5. Secure remote access through the use of firewalls, virtual private networks, etc.
6. Deactivate user accounts immediately upon separation from the District.

E. Safeguard from Unauthorized Physical Access.

1. All locations with network, SCADA, electronic devices, etc. shall be locked at all times and monitored by alarms (motion, door latch, camera, etc.).
2. Hardware is to be stored in a lock facility or to be locked in place.
3. Disable or password protect USB ports.
4. Secure documents with IT configuration information and passwords should be physically stored and locked. Electronic versions shall be password protect.

F. Install an Independent Cyber-Physical Safety System.

1. Review all cyber related functions and determine appropriate physical design elements that can be incorporated to limit or stop cyber-attacks.
   - (a) Use an independent monitoring system.
   - (b) Incorporate physical failsafes
2. Implement physical testing and calibration of critical equipment to ensure outside cyber threats are not impacting readings.

G. Embrace Vulnerability Management.

1. Create a culture of vulnerability awareness and action.
2. Once the vulnerability is identified implement the solution as soon as possible.
3. Attend trainings and conferences to stay current on the best cyber-hygiene practice.

4. Annual staff trainings on cybersecurity.
5. The General Manager shall commit to continuous improvement and enforcement of cybersecurity.

H. Plan for Incidents, Emergencies and Disasters.
   1. Obtain cybersecurity insurance.
   2. Create a disaster response plan for all cyber and electrical components.
   3. Power harden facilities so that all critical facilities have back-up power sources.

I. Secure the Supply Chain.
   1. Ensure background checks have been performed on all vendors that have access to cyber infrastructure (hardware & software).
   2. Require 3rd party security and vulnerability assessments on all software.

J. Participate in Information Sharing and Collaboration Communities.
   1. Report cybersecurity incidents to WaterSAIC (www.watersaic.org).
   2. Stay informed via the American Water Works Association's Water Infrastructure conference and associated committees.