Policy 4.28

EFFECTIVE 24 JAN 2023

SUPERSEDES 08 DEC 2020

CYBERSECURITY

IT IS THE POLICY OF THE EAST BAY MUNICIPAL UTILITY DISTRICT TO:

Protect the District's information and operational technology (IT and OT) environments through a proactive cybersecurity program that ensures the District can provide safe and reliable water and wastewater services.

Purpose

Identifying and managing cybersecurity risk in an increasingly connected and collaborative world is a critical part of the District's mission to deliver high quality water and wastewater services. The purpose of this policy is to ensure appropriate stewardship of all District IT and OT environments, including business systems as well as industrial control systems, network infrastructure, and data.

Objectives

- Maintain an organizational structure that monitors, reviews, and oversees cybersecurity across the District's IT and OT environments.
- Deliver effective cybersecurity procedures, standards, services, and solutions that balance the security and business needs of the District.
- Maintain effective physical security controls.
- Identify and implement mitigation strategies for minimizing cybersecurity risk.
- Continually improve cybersecurity capabilities to stay ahead of evolving cyber threats.
- Protect the confidentiality, integrity, and availability of all District data and IT and OT resources.
- Incorporate cybersecurity in the lifecycle of all IT and OT environments and software projects.
- Securely configure and maintain all District IT and OT environments, software, and network infrastructure.
- Prepare for, detect, and respond to cybersecurity incidents.
- Utilize a governance process for ensuring the cybersecurity program aligns with the District's business needs.
- Comply with all applicable federal, state, and local laws and regulations for cybersecurity and privacy.
- Implement and maintain appropriate Center for Internet Security Critical Security Controls for IT environments.
- Follow the National Institute of Standards and Technology Cybersecurity Framework methodology for OT environments.
- Complete periodic assessments of the cybersecurity program for IT and OT environments.
- Create a culture of cybersecurity awareness with all District employees, consultants, and contractors through applicable training and exercises.
- Enhance risk management by effectively communicating cybersecurity risks to District leadership and stakeholders.

Responsibilities

The Information Systems Department is responsible for executing cybersecurity policy in the IT environment and will work collaboratively with all District departments to provide guidance and assistance on implementing effective cybersecurity strategies to secure the District's IT and OT environments. The Operations and Maintenance, Engineering and Construction, and Wastewater departments are responsible for supporting and executing all cyber security measures in their respective OT environments. All District departments have a responsibility to support efforts to protect District technology resources.

Authority

Resolution No. 35209-20, December 8, 2020
As amended by Resolution No. 35335-23, January 24, 2023

References

Policy 4.20 – Use of District Technology Resources
Policy 7.03 – Emergency Preparedness/Business Continuity
Policy 7.13 – Workplace and Facility Security
Procedure 453 – Information Technology Use and Privacy
Procedure 461 – Information Technology Security
Procedure 466 – Personally Identifiable Information (PII) Data Security
Information Systems Department - Information Technology Standards
Center For Internet Security – Critical Security Controls
National Institute of Standards and Technology Cybersecurity Framework