THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

INFORMATION TECHNOLOGY SECURITY UNIT MANAGER

(Information Security Officer)

Group-Section: Information Technology Group	**FLSA Status:** Exempt **Bargaining Unit:** MAPA	**Salary Grade:** 68 **Job #:** UM032

JOB SUMMARY

The Information Security Officer (ISO) is responsible for establishing and maintaining a corporate-wide information security management program to ensure that information assets are adequately protected. The information assets at Metropolitan includes Standard Information Technology (IT) environments such as financial, human resources, engineering & facility maintenance systems and mission critical systems such as real time treatment plants operation, conveyance, distribution, and water quality monitoring detection and remediation systems.

OVERSIGHT

Oversight Received: Receives direction from a Section and/or Group Manager.

Oversight Given: May exercise technical and functional supervision over assigned and matrixed staff.

JOB DUTIES

1. Develops, implements, and monitors a strategic, comprehensive enterprise information security and IT risk management program to ensure that the integrity, confidentiality and availability of information is owned, controlled or processed by the organization.

2. Develops, maintains, and publishes up-to-date information security policies, standards, and guidelines. Oversees the approval, training, and dissemination of information security policies and practices. Creates and manages information security and risk management awareness training programs for all employees, contractors, and approved system users.

3. Creates, communicates, and implements a risk-based process for vendor risk management, including assessment and treatment for risks that may result from partners, consultants, cloud services and other service providers.

4. Provides regular reporting on the current status of the information security program to senior Metropolitan business leaders and the Board of Directors as part of a strategic enterprise risk management program.

5. Creates a framework for roles and responsibilities with regard to information ownership, classification, accountability, and protection. Develops and enhances an information security management framework based on national standards such as, ITIL (a set of best practice publications for IT service management), and National Institute of Standards and Technology (NIST). Creates and manages a unified and flexible control framework to integrate and normalize the wide variety and ever-changing requirements resulting from global laws, standards and regulations.

6. Provides strategic risk guidance for IT projects, including evaluation and recommendation of technical controls. Ensures that security programs are in compliance with relevant laws, regulations, and policies to minimize or eliminate risk and audit findings.

7. Liaises with the Enterprise Architecture Team to ensure alignment between the security and enterprise architectures, thus coordinating the strategic planning implicit in these architectures. Understands and interacts with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems, and services, including, but not limited to, privacy, risk management, compliance, and business continuity management.

8. Coordinates information security and risk management projects with resources from the IT organization and business units and teams.

9. Liaise amongst the information security team and corporate compliance, Audit Department, Legal Department, and Human Resources Group management as required.

10. Defines and facilitates the information security risk assessment process, including the reporting and oversight of treatment efforts to address negative findings. Manages security incidents and events to protect corporate IT assets, including intellectual property, regulated data and the District's reputation. Monitors the external threat environment for emerging threats, and advises relevant stakeholders on the appropriate courses of action. Liaises with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure that the organization maintains a strong information security posture.

11. Coordinates the use of external resources involved in the information security program, including, but not limited to, interviewing, negotiating contracts and fees, and managing external resources.

12. Facilitates a metrics and reporting framework to measure the efficiency and effectiveness of the program, facilitate appropriate resource allocation, and increase the maturity of the security.

13. Understands and interacts with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems and services, including, but not limited to, privacy, risk management, compliance and business continuity management.

14. Performs legislative reviews and analysis on cyber security proposed bills and executive orders.

15. Serves as the cyber security lead representative for the Metropolitan's North American Electric Corporation/ Western Electricity Coordinating Council (NERC/WECC) Compliance Program or its successor.

16. Performs other related job duties as required.

EMPLOYMENT STANDARDS

MINIMUM QUALIFICATIONS

Education and Experience: Bachelor's degree from an accredited college or university and twelve years of increasingly responsible relevant experience, of which four years must have been in a management or supervisory position; or an advanced degree from an accredited college or university and ten years of increasingly responsible relevant experience, of which four years must have been in a management or supervisory position.

Required Knowledge of: Information security and risk related concepts; principles and practices of maintaining secure computing environment; information security management frameworks, such as International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, ITIL, Control Objectives for Information and Related Technologies (COBIT), and ones from NIST; principles and practices of system design, development, and implementation; principles and practices of intrusion detection, firewall software, and antiviral software and practices of intrusion recovery; supervisory methods and techniques; team building; contract administration; project management including planning, scheduling, and costing; report writing; personnel management practices; practices and principles of strategic planning; performance measurement tools and metrics; policies and procedures related to budget, procurement, and human resources; programming theory and design; and basic understanding of Microsoft and UNIX operating systems.

Required Skills and Abilities to: Develop information security policies and procedures; manage a diverse work force; plan, organize, and review the work of subordinates; review work products for detail and adherence to guidelines; encourage, and facilitate cooperation; mentor, develop, and motivate staff; determine training needs of staff; exercise judgment and discretion; interpret and analyze information; communicate orally and in writing on administrative and technical topics; write, edit, and review action plans, and reports; research, evaluate, and implement new and emerging technologies; manage development of major applications and systems; evaluate total cost and return on investment for technology solutions; represent Metropolitan to public agencies, special interest groups, and members of the public; represent Metropolitan in negotiations with vendors; establish and maintain collaborative working relationships with all levels within the organization and use business applications; and prepare and make presentations on technical issues to peer forums, executive management, Board of Directors, member agencies, and regulatory agencies.

Certificates, Licenses, and Registrations Requirements

Certificates

- None

Licenses

- Valid California Class C Driver License that allows you to drive in the course of your employment

Registrations
- None

DESIRABLE QUALIFICATIONS
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- or other similar credentials

PHYSICAL DEMANDS, WORK ENVIRONMENT AND VISION REQUIREMENTS
The physical demands and work environment characteristics described here are representative of those that must be met or may be encountered by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Physical Demands: The work is sedentary. Typically, the employee may sit comfortably to do the work. However, there may be some walking; standing; bending; carrying of light items such as paper, books, or small parts; driving an automobile, etc. No special physical demands are required to perform the work.

Work Environment: The work environment involves everyday risks or discomforts that require normal safety precautions typical of such places as offices, meeting and training rooms, libraries, and residences or commercial vehicles, e.g., use of safe work practices with office equipment, avoidance of trips and falls, observance of fire regulations and traffic signals, etc. The work area is adequately lighted, heated, and ventilated. The work environment may include some exposure to outside elements. May travel to various sites requiring overnight stay.

Vision Requirements: No special vision requirements