



THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

SENIOR INFORMATION TECHNOLOGY SYSTEM ADMINISTRATOR

Group-Section: Business Technology Group	FLSA Status: Non-Exempt Bargaining Unit: AFSCME	Salary Grade: 52 Job #: YA65
--	--	---

JOB SUMMARY

This is the advanced journey level position performing Senior Information Technology System Administrator job duties.

DISTINGUISHING CHARACTERISTICS

Positions at this level are recognized as technical specialist using initiative and resourcefulness in deviating from traditional methods or researching trends and patterns to develop new methods, criteria, or proposed new policies. Decisions regarding what needs to be done include interpreting data, planning of the work, or refining the methods and techniques to be used. The work involves established criteria; formulating projects; assessing program effectiveness; or analyzing variety of unusual conditions, problems, or questions. The work product or service may affect activities, or the operation of other organizations.

OVERSIGHT

Supervision Received: The supervisor sets the overall objectives and resources available. The employee and supervisor, in consultation, develop the deadlines, projects, and work to be done. At this level, the employee, having developed expertise in the line of work, is responsible for planning and carrying out the assignment; resolving most of the conflicts that arise; coordinating the work with others as necessary; and interpreting policy on own initiative in terms of established objectives. In some assignments, the employee also determines the approach to be taken and the methodology to be used. The employee keeps the supervisor informed of progress, potentially controversial matters, or far-reaching implications. Completed work is reviewed only from an overall standpoint in terms of feasibility, compatibility with other work, or effectiveness in meeting requirements or expected results.

Supervision Given: Acts as a lead. Coordinates and reviews work assignments of employees performing the same general work as the lead on a day-to-day basis. Responsibilities may involve solving problems and providing instructions on work procedures.

JOB DUTIES

GENERAL

1. Provides expertise in troubleshooting, monitoring, analysis, and documentation of systems and applications for tuning, consistent configuration, vulnerabilities, and optimization.
2. Assists with upgrades and patches to systems.
3. Executes disaster recovery plan for area of responsibility.
4. Assists in the design of systems related to the related discipline.
5. Performs other related Information Technology System Administrator job duties as required.

DATABASE ADMINISTRATION

1. Leads and develops the plans and instructions, determines configurations, capacity, and installs software related to the Database or Web.
2. Leads and develops the plans and instructions, determines configurations, capacity, and installs upgrades and patches related to the Database or Web.
3. Leads in developing and updating documents related to the Database or Web.
4. Leads in troubleshooting and debugging problems related to the Database or Web.
5. Leads the development and execution of Disaster Recovery plan for Database or Web.
6. Leads and prepares Database or Web requirements and develops Database or Web structures.
7. Leads and estimates time, resources, and scope related to Database or Web projects.
8. Leads and coordinates tasks and resources related to implementation of Database or Web projects.
9. Leads and performs researching and analyzing current trends in Database or Web technologies, tools, and best practices.
10. Leads and designs Database or Web architecture and standards to ensure data integrity, security, and availability.

SECURITY ADMINISTRATION

1. Leads and plans and designs security access for the infrastructure for internal and external environments.
2. Leads and plans and designs with the implementation of security measures for the hardware, software, and infrastructure for internal and external environments.
3. Leads and plans and configures of security interfaces for desktop, enterprise systems, and Web environments.
4. Leads the development and execution of Disaster Recovery plan for systems recovery.
5. Leads and identifies products and develops strategies for remediation and resolution of security issues and events.
6. Leads and performs security analysis, diagnosis and reporting for system security issues in support of audits.
7. Leads and performs researching and analyzing current trends in security technologies, tools, and best practices.
8. Leads and develops and updates documents related to the security environment.
9. Leads and develops the disaster recovery plan, and executes the plan for Information Security.

EMPLOYMENT STANDARDS

MINIMUM QUALIFICATIONS

Education and Experience: Bachelor's degree from an accredited college or university in a related field and six years of relevant experience; or Master's degree from an accredited college or university in a related field and four years of relevant experience.

General Required Knowledge of: Principles, practices, and procedures of Information Technology; principles of leadership and training; application, and peripheral equipment; principles and practices of system design, testing, analysis, data management and integrity; hardware and software configuration; operational characteristics of various computer systems; system administration for related discipline; project management; disaster recovery practices; and current office technology and equipment.

Database Administration Required Knowledge of: Principles, practices, and procedures of database and web administration; principles, practices, and procedures of data management and application software; principles of strategic leadership and training for database and web systems; operational characteristics of server operating systems; and methods and techniques to develop, test, and implement database or web application systems.

General Required Skills and Abilities to: Organize, and review work performed in area of discipline; analyze business requirements, design, test, and implement systems and solutions; analyze requests and provide customer assistance for solutions; maintain confidentiality for proprietary and personal information; use independent judgment and exercise discretion; problem solve; prioritize and multi-task; communicate clearly and concisely, both verbally and in writing; establish and maintain effective working relationships with those contacted in the course of work; work independently and in a team environment; lead and train; and operate current office equipment including computers and supporting applications.

Security Administration Required Knowledge of: Separation of duties in supporting creation of roles and responsibilities within applications and systems; directory or server interfaces for security levels; layered security methods; security methods for operating systems; security environments and requirements for applications; Network Security Monitoring and Incident Response operations; remediation methods; information technologies such as computer hardware and software, operating systems, and networking technologies; concepts of computer forensics; and highly available, mission critical, sensitive applications.

Database Administration Required Skills and Abilities to: Monitor and optimize database and web systems; install, configure and support database and web related software, upgrades, and patches; backup and recover database and web related systems; perform research and development in database and web technologies; and lead database and web enterprise projects.

Security Administration Required Skills and Ability to: Create roles in applications and systems using information security practices and standards; investigate and remediate cyber incidents; recommend configuration changes to improve security without degrading workflows; identify, analyze, remediate and report on cyber security incidents; analyze malware to determine direct threat to organization, maintain detailed incident logs, provide detailed procedures and standards documentation; and write reports to communicate incidents, issues and directions.

CERTIFICATIONS, LICENSES, AND REGISTRATION REQUIREMENTS

Employees in this position may be required to obtain and maintain the following certifications, licensing and registrations:

Certificates

- Valid Certified Information Systems Security Professional (For the Security Administrator at all levels.)
- Valid Certified Information Systems Auditor (For the Security Administrator at all levels.)

Licenses

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

Registrations

- None

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 job duties of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the job duties.

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.

Vision Requirements: No special vision requirements.