Midpeninsula Regional Open Space District

INFORMATION TECHNOLOGY ANALYST I/II

DEFINITION

Under general supervision (IT Analyst I) to direction (IT Analyst II) performs analysis and strategic support for the District's information technology systems, cybersecurity posture, and infrastructure; evaluates technology performance, identifies risks, and develops solutions to optimize efficiency, security, and compliance; serves as a technical advisor and project contributor, ensuring IT initiatives align with organizational goals and industry best practices; and performs related duties, as assigned.

SUPERVISION RECEIVED AND EXERCISED

Receives general supervision (IT Analyst I) to direction (IT Analyst II) from the Information Technology Program Manager. Exercises no direct supervision over staff.

CLASS CHARACTERISTICS

IT Analyst I: This is the entry-level classification in the IT Analyst series. Initially under close supervision, incumbents learn and perform routine systems analysis and support, while learning District policies and procedures. As experience is gained, assignments become more varied, complex, and difficult; close supervision and frequent review of work lessen as an incumbent demonstrates skill to perform the work independently. Positions at this level usually perform most of the duties required of the positions at the IT Analyst II-level but are not expected to function at the same skill level and usually exercise less independent discretion and judgment in matters related to work procedures and methods. Work is usually supervised while in progress and fits an established structure or pattern. Exceptions or changes in procedures are explained in detail as they arise.

IT Analyst II: This is the journey-level classification in the IT Analyst series. Positions at this level are distinguished from the IT Analyst I-level by the performance of the full range of duties as assigned, working independently, and exercising judgment and initiative. Positions at this level receive only occasional instruction or assistance as new or unusual situations arise and are fully aware of the operating procedures and policies of the work unit. This class is distinguished from the Senior IT Analyst in that the latter performs the more complex work assigned to the series and provides technical and functional direction over lower-level staff.

Positions in the IT Analyst class series are flexibly staffed; positions at the II-level are normally filled by advancement from the I-level; progression to the II-level is dependent on (i) management affirmation that the position is performing the full range of duties assigned to the classification; (ii) satisfactory work performance; (iii) the incumbent meeting the minimum qualifications for the classification including any licenses and certifications; and (iv) management approval for progression to the II-level.

EXAMPLES OF TYPICAL JOB FUNCTIONS (Illustrative Only)

Management reserves the right to add, modify, change, or rescind the work assignments of different positions and to make reasonable accommodations so qualified employees can perform the essential functions of the job.

Positions at the IT Analyst I-level may perform some of these duties and responsibilities in a learning capacity.

- Audits, analyzes, and optimizes IT systems and workflows to improve efficiency, security, and user experience.
- Administers assigned cloud and Software as a Service (SaaS) platform; monitors service performance and availability, implements new features, optimizes workflows, automates routine tasks, and manages user access and digital resources.
- Provides advanced escalation support; triages high-impact or unprecedented issues, develops action plans, assigns permissions, and authors reference runbooks and guides for the IT team.
- Develops and implements identity and access management strategies; ensures compliance with organizational security policies.
- Monitors cybersecurity posture; analyzes alerts and logs, investigates user-reported threats, and implements mitigations through policy or configuration changes; administers and operates enterprise cybersecurity platforms including Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and email security systems.
- Performs end-to-end incident response including investigation, containment, remediation, and post-incident reporting; reviews and enhances email security protocols; develops strategies to mitigate phishing and other threats.
- Designs and enforces authentication and access control frameworks, including multi-factor authentication and conditional access.
- Develops governance and compliance frameworks for data protection; monitors adherence and recommends improvements.
- Participates in maintaining enterprise mobile device management systems and associated hardware/software across multiple platforms; supports administration of telecommunications accounts and services, ensuring continuity and cost-effectiveness.
- Participates in maintaining and upgrading server and network infrastructure, including virtualized environments and enterprise applications.
- Participates in development processes and systems to ensure the backup and security of the District's database systems; works with departments and management to develop database security and recovery policies and procedures.
- Oversees assigned virtualized infrastructure and enterprise applications; ensures operational functionality, monitors performance, applies updates, and remediates cybersecurity vulnerabilities.
- Researches and implements automation solutions to streamline IT operations and security processes.
- Analyzes network infrastructure performance; recommends configurations for firewalls, switches, wireless systems, and virtualization platforms.
- Configures, administers, and maintains firewalls, network switches, wireless systems, and virtualized environments; performs updates, security configurations, and troubleshooting.
- Plans, scopes, and designs technology solutions for new or remodeled workspaces and meeting rooms; coordinates requirements and implementation with facilities and project stakeholders.
- Develops proactive maintenance strategies based on trend analysis and predictive indicators.
- Creates and maintains technical documentation and process standards; ensures accuracy and usability for stakeholders.
- Provides guidance and mentorship to technical staff; develops training plans and knowledge-sharing initiatives.
- Collaborates with vendors and internal stakeholders to evaluate technology solutions; provides procurement analysis and recommendations.
- Contributes to budget recommendations for technology purchases and replenishment of IT supplies within delegated limits.

- Leads or contributes to IT projects by defining requirements, analyzing risks, and ensuring alignment with organizational goals.
- Monitors emerging technologies and cybersecurity developments; assesses applicability and prepares adoption strategies.
- Evaluates, tests, and implements AI-driven tools that enhance cybersecurity, automation, system performance, or user experience.
- Observes and complies with all District and mandated safety rules, regulations, and protocols.
- Performs other duties as assigned.

QUALIFICATIONS

Knowledge of:
Positions at the IT Analyst I-level may exercise some of these knowledge and abilities statements in a learning capacity.

- Principles and practices for auditing, analyzing, and optimizing IT systems and workflows for efficiency, security, and user experience.
- Administration of cloud and SaaS platforms, including service monitoring, feature implementation, workflow optimization, and resource assignment.
- Troubleshooting techniques for high-impact or unprecedented technical issues and escalation management.
- Identity and access management concepts, including policy design, compliance standards, and lifecycle management.
- Cybersecurity fundamentals, including threat analysis, log interpretation, and mitigation strategies.
- Authentication and access control frameworks, including multi-factor authentication and conditional access policies.
- Data governance principles, compliance frameworks, and risk management strategies.
- Virtualization technologies and enterprise application hosting, including performance monitoring and update processes.
- Automation and scripting techniques for IT operations and security tasks.
- Network infrastructure design and performance analysis, including firewalls, switches, wireless systems, and virtualization platforms.
- Standards for technical documentation, process development, and knowledge-sharing practices.
- Project management principles, including requirements definition, risk analysis, and alignment with organizational goals.
- Applicable federal, state, and local laws, codes, and regulations as well as industry standards and best practices pertinent to the assigned area of responsibility.
- District and mandated safety rules, regulations, and protocols.
- Techniques for providing a high level of customer service by effectively dealing with the public, vendors, contractors, and District staff.
- The structure and content of the English language, including the meaning and spelling of words, rules of composition, and grammar.
- Modern equipment and communication tools used for business functions and program, project, and task coordination, including computers and software programs relevant to work performed.

Ability to:

- Audit, analyze, and optimize IT systems and workflows to improve efficiency, security, and user experience.
- Administer cloud and SaaS platforms; monitor performance and availability, roll out new features, streamline workflows, and manage resource allocation.

- Provide advanced escalation support; triage complex issues, develop action plans, and create reference documentation.
- Develop and implement identity and access management strategies; ensure compliance with security policies.
- Monitor cybersecurity posture; analyze alerts and logs, investigate threats, and apply mitigation measures.
- Design and enforce authentication and access control frameworks, including multi-factor authentication and conditional access.
- Develop governance and compliance frameworks for data protection; monitor adherence and recommend improvements.
- Research, develop, and implement automation solutions to streamline IT operations and security processes.
- Analyze network infrastructure performance; recommend configurations for firewalls, switches, wireless systems, and virtualization platforms.
- Create and maintain technical documentation and process standards.
- Contribute to budget planning for technology purchases.
- Use tact, initiative, prudence, and independent judgment within general policy, procedural, and legal guidelines.
- Independently organize work, set priorities, meet critical deadlines, and follow-up on assignments.
- Effectively use computer systems, software applications relevant to work performed, and modern business equipment to perform a variety of work tasks.
- Communicate clearly and concisely, both orally and in writing, using appropriate English grammar and syntax.
- Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

Education and Experience:
Any combination of training and experience that would provide the required knowledge, skills, and abilities is qualifying. A typical way to obtain the required qualifications would be:

Education:

IT Analyst I/II:
- Equivalent to a bachelor's degree from an accredited college or university with major coursework in computer science, information technology, or a closely related field.

Experience:

IT Analyst I:
- One (1) year of professional experience or two (2) years of technical experience supporting a comprehensive information technology program.

IT Analyst II:
- Two (2) years of increasingly responsible experience supporting a comprehensive information technology program equivalent to the IT Analyst I with the District.

Licenses and Certifications:

- Possession of a valid California Driver's License to be maintained throughout employment.

PHYSICAL DEMANDS

Must possess mobility to work in a standard office setting and use standard office equipment, including a computer; to operate a motor vehicle and visit various district sites; vision to read printed materials and a computer screen, as well as interpret colored warning and alarm lights on computer equipment; and hearing and speech to communicate in person and over the telephone. This is primarily a sedentary office classification although standing in work areas and walking between work areas may be required. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Positions in this classification occasionally bend, stoop, kneel, reach, push, and pull drawers open and closed to retrieve and file information. Employees must possess the ability to lift, carry, push, and pull materials and objects up to 40 pounds.

ENVIRONMENTAL CONDITIONS

Employees work primarily in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances. Employees may be required to travel to District field sites where exposure to loud noise levels, cold and hot temperatures, inclement weather conditions, road hazards, vibration, and mechanical and/or electrical hazards are possible. Employees may interact with upset staff and/or public and private representatives in interpreting and enforcing divisional policies and procedures.

EFFECTIVE: October 2026
REVISED:
FLSA: Non-Exempt/Exempt