JOB TITLE:	SENIOR INFORMATION SYSTEMS MANAGER	DIVISION:	DISTRICT – INFORMATION SYSTEMS
REPORTS TO:	CHIEF TECHNOLOGY DIRECTOR	EEO CATEGORY:	02-PROFESSIONAL
FLSA:	EXEMPT	SAFETY-SENSITIVE:	NO
CLASSIFICATION:	NON-REPRESENTED	LOCATION:	SAN FRANCISCO

Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are not intended to reflect all duties performed within the job.

Position Summary

Under the general direction of the Chief Technology Director, the Senior Information Systems (IS) Manager, manages, coordinates and supervises various professional, technical and analytical staff and duties associated with application development, Technical Services, and Enterprise projects. The operation of information systems including internet, network, and desktop computer systems; the position oversees the analysis, design, acquisition, implementation and/or maintenance of related systems hardware, software and/or programs; she/he shall also protect ISD business systems and ISD computer networks from cyberattacks, intrusions, malware and various types of data breaches. In addition, position shall provide assistance to administrative staff; and maintain good working relationship with District customers, internal IS staff and with third-party system suppliers.

Essential Responsibilities

- Plans, organizes and directs, often through subordinate supervisors, the work of staff engaged in the analysis, design, implementation, programming, support and/or maintenance of information systems including internet, network, client/server and/or desktop computer systems; coordinates the acquisition of hardware, software and related equipment; provides broad operational oversight in area(s) of assignment.
- Assures that production schedules and project deadlines are met; establishes work priorities and develops cost analyses; may serve as a project manager for both small and large scale projects; may coordinate and/or perform feasibility studies.
- Performs complex analytical studies; oversees the production of statistical, data and/or narrative reports and other documents.
- Assists with Department policy development and implementation; researches and evaluates advances in information technology hardware and software including internet and/or web technology; develops and recommends District-wide standards for product evaluation and selection; reviews and recommends capital budget requests for equipment, staff and services; participates in department budget preparation.
- Oversees system testing and quality control; meets and consults with customers and vendors regarding service delivery needs; coordinates problem solving, conflict resolution, escalations; responsible for disaster recovery; serves as technical resource for identifying complex problems with systems hardware, software and/or programs.

- Conducts planning and implementing security measures on all information systems and ISD-managed corporate networks. Establishes network security policies and procedures, regulating access to information and training staff on proper use of information systems; Monitors systems for security gaps, designs effective solutions and provides reports to management and executive staff; runs risk assessments, tests ta processing systems and designs firewalls; responds to and takes care of an intrusion if it does take place; responsible for coordinating, supervising, managing, and training IS and/or District employees for cyber security.
- Monitors operations, infrastructure, and business applications for any potential cyberattacks. Keeps an eye on organization's digital security footprint by monitoring alerts and logs (the computer security equivalent of video surveillance) in person and/or with consultants' help.
- Manages the maintenance of cyber security tools and technologies.
- Monitors internal and external policy compliance. Ensures that both vendors and employees understand cybersecurity risk management policies and that they operate within that framework by making sure things are in line internally.
- Monitors regulation compliance. Tackles the need for compliant issues with District's systems and data at all levels. This includes, PCI compliance, HIPPA compliance, NIST framework compliance, and other compliance requirements. Signs compliance paperwork as needed.
- Works with different departments in the organization to reduce cyber risks. From technical controls to policies, works across departments in the organization to reduce cyber risks for both our IS-managed network infrastructure and business applications deployments.
- Details out the security incident response program. Forms a well-defined and documented plan of action to put into place if a security incident does occur.
- Oversees staff development and training in assigned areas; may develop and/or present District wide training programs on information technology issues; may perform training-related needs assessments and recommend County-wide training plans.
- Schedules and attends staff meetings; may serve on committees and task forces.
- Performs additional related duties as assigned
- Regular and reliable attendance and performance is required

Required Knowledge, Skills and Abilities

Working knowledge of:
- District policies and applicable Memorandum of Agreement (MOU)
- Current developments, equipment, technology and methods of administering a broad program of information systems and services
- Cyber security related policies, procedures and best practices, standards and guidelines as applied to the District's business.
- Cyber Incident Response best-practice process and requirements.
- Project management theory, concepts and principles (e.g., theory of constraints, critical path methodology, project risk management, project scope management, project management life cycle, etc.)
- Project management tools and/or software packages
- Strategic, operational and technical & management skills

- Excellent communication, leadership, problem solving and analytical skills

<u>Ability to:</u>
- Maintain current in the IT and Cyber security domains related to researching emerging cyber security threats, trends and technology to formulate enhanced solutions for the customer
- Conduct needs analysis, develop technical specifications, issue requisite procurement and budgetary documentation, plan, develop, test, and implement technology systems to improve operations and create efficiencies
- Demonstrate leadership managing people, including the ability to work and lead in project teams
- Work independently and manage multiple task assignments but also experience working in a team-oriented, collaborative environment
- Rapidly adapt and respond to changes in environment and priorities
- Elicit cooperation from senior management and other departments
- Demonstrate experiences leading outsourced providers and maintaining partnerships with key vendors
- Analyze, evaluate, and problem solve and comfortable with ambiguity
- Work independently, show initiative, and effectively prioritize work
- Maintain good working relationship with users, internal Information Systems Department and with system software and hardware suppliers
- Effectively train a variety of users at different levels of knowledge and expertise
- Establish and maintain effective working relationships with District personnel, contractors, vendors and others
- Follow the safety and health rules and safe working practices applicable to the job

Minimum Qualifications

Education and/or Experience:
- Bachelor's degree in Computer Science, Information Systems, Software Engineering, Computer Engineering or other related technology major. Applicants who do not possess a degree should attach a statement supporting qualifying certifications and experience.
- A minimum of six (6) years Information Systems experience and three (3) years of management experience leading IS teams and large scale enterprise projects that requires fundamental change in business practice and automation to deliver significant value to business.
- **PMI Certification is highly desirable.** Applicants who do not possess a certification should attach a statement supporting recent qualifying experience.

Required License: Must possess and maintain a current, valid California driver's license and satisfactory driving record. May operate District vehicles.

Physical Requirements: Mobility to work in a typical office setting. Ability to communicate in person and over the telephone. Ability to read printed materials and a computer screen. Ability to travel to District facilities. Routine use of computer, telephone and other office equipment. May require some weekend and evening work.