CYBERSECURITY MANAGER

DEFINITION

Under direction, maintains a safe and secure information systems and network environment for customers and employees, provides vision and leadership for developing and supporting security initiatives. Supervises staff and contractors assigned to implement and maintain the citywide information and communications systems.

SUPERVISION RECEIVED/EXERCISED

Receives supervision from Chief Information Officer (CIO) or designee. Exercises supervision over assigned staff.

DISTINGUISHING CHARACTERISTICS

The Cybersecurity Manager functions as the advisor for all new or existing enterprise associated software, hardware, communications, or network elements within the City as it pertains to security. The incumbent supervises and provides leadership to assigned staff; manages the security of data communications systems including local and wide area networks, communication systems, internet and intranet systems, and applications software; and is responsible for the security of the City's technology systems. This is an unclassified position in which the incumbent serves at the will of the Department Director.

EXAMPLES OF IMPORTANT AND ESSENTIAL DUTIES

May include, but are not limited to, the following:

Plans, organizes and manages the activities of the Cybersecurity Division; plans coordinates, administers, and evaluates projects, processes, procedures, systems and standards; develops and coordinates work plans.

Participates in the development and implementation of goals, objectives, policies, and priorities for assigned programs; recommends and administers policies and procedures.

Plans, manages, coordinates, and reviews the work plan for assigned staff; assigns work activities, projects, and programs; reviews and evaluates work products, methods, and procedures; meets with staff to identify and resolve problems.

Selects, trains, motivates, and evaluates assigned personnel; provides or coordinates staff training; works with employees to correct deficiencies; implements discipline and termination procedures.

Develops, implements and monitors a strategic, comprehensive enterprise information security and IT risk management program; partners with stakeholders to raise awareness of risk management concerns.

Develops and enhances an information security management framework.

Understands and interacts with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems and services.

Assists with the overall business technology planning, providing a current knowledge and future vision of technology and systems; schedules and assists with resource implementation.

Provides insight and analysis of long-term and short-term planning in relation to any information technology processes within entities on security.

Assists in planning and organizing technical and functional requirements associated with major or minor electronic, software or network releases, cyber security systems or impacting changes.

Identifies new developments in all enterprise-associated programs, policies and procedures.

Performs other duties as assigned.

JOB RELATED AND ESSENTIAL QUALIFICATIONS

Knowledge of:

Technology environments, including information security, building security, and defense solutions.

Business theory, business processes, management, budgeting, and business office operations.

Computer systems characteristics, features, and integration capabilities.

Systems design and development from business requirements analysis through to day-to-day management.

Principles and practices of project management.

Data processing, hardware platforms, enterprise software applications, and outsourced systems.

Applicable laws and regulations as they relate to security.

Principles and practices of program development and administration.

Principles of supervision, training, and performance evaluation.

Ability to:

Apply IT while solving security problems.

Plan, organize, and develop IT security and facility security system technologies.

Plan and execute security policies and standards development.

Select, train, and evaluate staff.

Oversee and participate in the development and administration of division goals, objectives, and procedures.

Plan, organize, direct and evaluate the work of contractors.

Coordinate, facilitate, motivate and empower subordinate personnel to accomplish the division's mission.

. **Skill to:**

Operate a motor vehicle safely.

MINIMUM QUALIFICATIONS

Graduation from an accredited college or university with a bachelor’s degree in business administration, public administration, computer science, electronics, electrical or communications engineering or related field;

AND

Three (3) years of experience in communications or computer systems technology involving cyber security, maintenance and operation of complex computer systems hardware and software or communications equipment, which includes or is supplemented by, one (1) year of lead or supervisory experience. Additional qualifying experience may be substituted for the required education on a year-for-year basis, up to a maximum of two (2) years.

Certified Information Systems Security Professional (CISSP) and/or Certified Information Security Manager certifications is desired.

Special Requirements:
Possession and continued maintenance of a valid California Driver's License is required at time of appointment.

APPROVED: *(Signature on File)* DATE: 7/7/21
Director of Personnel Services

NEW: JTC:SCM:bn