CITY OF CARLSBAD
CLASS SPECIFICATION

JOB TITLE: **INFORMATION TECHNOLOGY SECURITY MANAGER**

DEPARTMENT: **INFORMATION TECHNOLOGY**

BASIC FUNCTION/DISTINGUISHING CHARACTERISTICS:

Under general direction, plans, organizes, oversees, coordinates, reviews, and implements all aspects of citywide information security and cybersecurity programs that are designed to provide the protection and confidentiality of data, along with protection of other systems and assets of the City of Carlsbad; defines, documents, and implements cybersecurity strategies, architectures, and procedures, and verifies that all data and computing infrastructure is properly protected from internal and external threats; coordinates assigned activities with other city IT staff, departments, divisions, outside agencies and the general public; and performs related work as assigned.

DISTINGUISHING CHARACTERISTICS:

This is a single mid-management classification in the Information Technology Department that manages cybersecurity related activities. The incumbent oversees and administers the day-to-day program, budgetary, and administrative activities for assigned security programs. Responsibilities include development, maintenance, and design of security policy as well as security education, training, and awareness activities.   The incumbent is accountable for accomplishing departmental planning and operational goals and objectives and for furthering city goals and objectives within general policy guidelines.

KEY RESPONSIBILITIES:

- Responsible for development, documentation, and maintenance of information security policies, procedures, and standards for the city.
- Performs routine (daily, weekly, periodic) monitoring of changes in local, state, and federal regulations and accreditation standards related to security; coordinates activities with corresponding agencies to ensure security compliance measures.
- Establishes and enforces standards, procedures, and/or policies in support of up-to-date security internal controls.
- Makes recommendations for selecting and implementing security-based hardware and software solutions; provides security interpretation and/or training, security education, and awareness to users as needed.
- Acts as a liaison with internal user departments by providing analysis, consultation, assistance, and troubleshooting of related security activities; develops reports of findings, alternatives, and recommendations.
- Leads the creation, maintenance and implementation of the information systems disaster recovery and business continuity plans and procedures.
- Tests, monitors, and performs regular analysis of the effectiveness of the city's security tools and incident response measures; defines user access levels and protocol for potential data breech.

- Coordinates, investigates, and reports on cyber security incidents; manages and implements recommendations for incident response and assists in policy development for data threat strategies and security tools.
- Implements training programs and prepares user guides in for cyber security.
- Manages and participates in the development and implementation of goals, objectives, policies and priorities for assigned security programs; recommends within departmental policy, appropriate service and staffing levels; recommends and administers policies and procedures.
- Develops and standardizes procedures and methods to improve the efficiency and effectiveness of assigned areas of operation; continuously monitors and evaluates the service delivery methods and procedures and identifies opportunities for improvement; recommends improvements and implements new procedures and methods.
- Manages consultants and contractors working on information technology related projects specifically in the area of security services
- Monitors changes in regulations and technology that may affect operations; implements policy and procedural changes after approval; updates city records and procedures in assigned areas pursuant to changes in law, city policies and procedures, and other pertinent rules and regulations.
- Attends and participates in professional group meetings; stay abreast of new trends and innovations in the field of information technology; research emerging products and enhancements and their applicability to city needs.
- Participates as a technical expert in the negotiation of Information Technology contracts.
- Manages and executes technology projects including special projects, such as technology upgrades for facilities that are being remodeled, etc.
- Assists in the implementation of information and telecommunication systems in accordance with city policy and laws pertaining to privacy and system security.
- Maintain and monitor SIEM platform to identify cyberthreats in the computing environment
- Conduct regular vulnerability assessments
- Acts as a liaison or project manager with contracting agencies.
- Performs other duties as assigned.

QUALIFICATIONS:

Knowledge of:

- Administrative principles and practices, including goal setting, program development, implementation and evaluation, project management, and supervision of staff, either directly or through subordinate levels of supervision.
- Principles, practices, and programs related to information security best practices, procedure, risk assessment, methodologies, and vulnerability.
- Information security frameworks, software, hardware, and technologies.
- Current information security compliance standards and regulations.
- Current and emerging security tools, techniques, and programs.
- Innovative problem solving techniques and practices.
- Principles and practices of budget administration.
- Principles and practices of employee supervision, including work planning, assignment, review and evaluation and the training of staff in work procedures.

- Information technology systems, software, database management, policies and procedures, including computer networks, security, mini-computers, telecommunications, copiers and other electronic office automation systems.
- Operating systems such as Microsoft, Linux, Mac operating systems, local and wide area communications networks, and software applications.
- Operating principles and practices of desktop and server hardware and software related to the establishment and maintenance of internal and external networks.
- Principles and practices of application development methodologies and programming languages.
- Terminology, methods, techniques and practices of the operation and maintenance of network and personal computer hardware and software, including word processing, spreadsheet, database, and graphics applications.
- Applicable federal, state, and local laws, codes and regulations concerning the operation of computer systems and networks.
- Principles and practices of contract facilitation, negotiation, administration, and evaluation.
- Organization and management practices as applied to the development, analysis and evaluation of information technology programs, policies and operational needs.
- Occupational hazards and standard safety practices necessary in the area of computer operations.
- Techniques for effectively representing the city in contacts with governmental agencies, community groups, various business, professional, educational and regulatory organizations and with property owners, developers, contractors and the public.
- Techniques for dealing effectively with the public, vendors, contractors and city staff, in person and over the telephone.
- Techniques for providing a high level of customer service to the public and city staff, in person and over the telephone.
- Safe work practices.

Abilities:

- Administering information security programs including assessing, developing, implementing, maintaining, and evaluating.
- Prioritizing and responding expeditiously to data threats or policy deviations.
- Advising on the acquisition, design and construction of computer systems and other related equipment.
- Applying technology at a strategic and system's level to solve business problems.
- Analyzing findings, making recommendations and preparing reports; maintaining organized and detailed records; organizing work, coordinating projects; setting priorities, objectives, policies, and procedures, meeting critical deadlines and following-up on assignments with minimum direction.
- Managing responsibilities including delivering, managing and supporting complex projects on-time and within budget.
- Preparing clear and concise reports, correspondence, policies, procedures and other written materials.
- Presenting technical information orally and in writing in a non-technical way for employees, community groups and decision-makers.
- Interpreting, explaining, and ensuring compliance with city policies and procedures.
- Presenting technical information orally and in writing in a non-technical way for employees, community groups, and decision-makers.

- Analyzing and presenting recommendations to city management on vendor products and services.
- Using English effectively to communicate in person, over the telephone and in writing.
- Establishing and maintaining effective working relationships with those contacted in the course of the work.
- Operating, installing, maintaining, configuring, and troubleshooting a variety of highly technical computer equipment and peripherals.
- Operating a motor vehicle safely.

EXPERIENCE AND EDUCATION:

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:

Equivalent to graduation from an accredited four-year college or university with major coursework in computer science, information security, or a related field, and five (5) years of experience in managing security for an organization.

Possession of Certified Ethical Hacker (CEH) and Certified Information Systems Security Professional (CISSP) certifications are preferred.

PHYSICAL REQUIREMENTS AND ENVIRONMENTAL SETTING:

- Needs to be able to operate equipment and machinery with some requiring rapid adjustments such as a computer keyboard and terminal, printers, photocopier and calculator. Must be able to coordinate eyes, hands, feet and limbs in performing skilled movements such as rapid keyboard use. Needs to be able to recognize and identify degrees of similarities or differences between characteristics of colors, textures, and forms associated with job-related objects, materials, and tasks.
- Essential and marginal functions may require maintaining physical condition necessary for sitting for prolonged periods of time. Must be able to exert light physical effort, typically involving lifting, carrying, pushing and pulling of up to 15 pounds. Tasks may involve extended periods of time at a keyboard or workstation. Needs to be able to perform frequent downward flexion of neck, side-to-side turning of the neck, fine finger dexterity and grasp to manipulate the keyboard, telephone, writing instruments, papers, books, manuals, and reports.
- Job entails occasional walking, standing, bending, stooping, climbing, and reaching at and above shoulders and twisting at the waist. On an infrequent basis, the incumbent must be able to squat and kneel.
- Overtime and attending meetings outside regular work hours may be required. Work environment is professional and both team and autonomy oriented. This position is impacted by urgent time deadlines due to various reporting and filing requirements. There is a need for extreme accuracy and paying attention to detail. Additionally, there is a need to be able to shift attention before tasks are completed to be able to balance user demands, telephone and other interruptions.
- Must be able to drive and maintain a California Class C Driver's license or ability to arrange transportation for fieldwork or visits to other city facilities when necessary.

This is an at-will management classification.

DATE APPROVED: July 3, 2019