CITY OF CARSON
Class Specification

City Council Reso. No: 24-005
Bargaining Unit: AME
FLSA: Exempt

INFORMATION TECHNOLOGY SECURITY OFFICER

Job Summary:

The purpose of this classification is to ensure the security operation of the City's data, computer systems, servers, and network connections. Employees in this classification are responsible for developing, planning, organizing, managing, implementing, maintaining, and performing cybersecurity risk analysis of systems; scrutinizing network traffic; establishing vulnerability scans; checking server and firewall logs; conducting user activity audits, and troubleshooting, as well as also analyzing and resolving security breaches and vulnerability issues in a timely and efficient manner This position will assist with developing IT security policies. Work is performed under general direction of the Director of Information and Technology with considerable latitude for the use of initiative and independent judgment.

Essential Duties and Responsibilities:

(These functions are representative and may not be present in all positions in the class. Management reserves the right to add, modify, change or rescind related duties and work assignments.)

- Plans, organizes, manages, and participates in the development, implementation, and monitoring of the City's information security programs, information technology risk management programs, and information security policies; supervises and reviews the work of professionals and serves as a subject matter expert in information security.
- Develops and executes a cyber security strategy that is aligned with internal stakeholders, organizational priorities, facilitates city operations, and meets industry standards.
- Directs and participates in the identification of security risks, development and implementation of security management practices, and the measurement and monitoring of security protection measures.
- Ensures compliance with regulatory requirements such as Criminal Justice Information Services (CJIS), Payment Card Industry Data Security Standards (PCI), Health Insurance Portability and Accountability Act (HIPAA), California Privacy Protection Agency, and federal, state, and local laws.
- Monitors agency infrastructure, devices, and information systems for security integrity; provides planning and guidance to information technology staff on vulnerability management and security incident response procedures.
- Oversees portfolio of cyber risk and security applications and procedures, implements new security processes and related technologies to ensure a continuous improvement of the City's cyber security posture.
- Oversees assigned staff in performing their responsibilities and provides guidance as necessary.
- Analyzes information, situations, problems, policies, and procedures to identify, recommend, and implement solutions systemically.
- Formulates, recommends, and executes enterprise-wide policies and procedures for detecting, deterring, and mitigating information security threats.
- Serves as a subject matter expert and internal consultant on data security implications for proposed information technology projects and programs and makes recommendations to align new technologies to security standards.
- Prepares oral and written reports for executive leadership, the City Manager's Office, and City Council.

- Develops cyber security, cyber risk, and security awareness training programs for City staff; monitors training effectiveness by documenting and reporting data point trends on user awareness and vulnerability assessments.
- Builds and maintains positive relationships with City stakeholders.
- Attends City/Industry-related functions.
- Performs other duties as required

Qualification Guidelines:

A typical way to obtain the requisite qualifications to perform the duties of this class is as follows:

Education and/or Experience:

Option A:
Bachelor's degree in Business Administration, Computer Information Systems, Information Technology or closely related field from an accredited college or university and five (5) years of paid experience performing IT security management; and at least two (2) years in an administrative or management capacity responsible for cyber security risk assessment, implementation of security management practices, monitoring of security protection measures, managing SIEM, vulnerability management, and other security tools in an enterprise environment.

Option B
Master's degree in Computer Science or closely related field is highly desirable from an accredited college or university and four (4) years of paid experience performing IT security management; and at least two (2) years in an administrative or management capacity responsible for cyber security risk assessment, implementation of security management practices, monitoring of security protection measures, managing SIEM, vulnerability management, and other security tools in an enterprise environment.

Knowledge of:

- Computers and Electronics: Electric circuit boards, processors, chips, and computer hardware and software
- Principles, methods, and practices of systems/network administration and maintenance.
- Agency policies and procedures and practices regarding data security.
- Network security design principles, practices, and related tools and software.

Skills and/or Ability to:

- Ability to objectively assess situations or circumstances using all the relevant information, apply experience, evaluate the problem objectively, calculate risks, and make an ethical and informed decision.
- Manage the performance of staff by coaching for performance.
- Motivating, developing, and directing people as they work.
- Acknowledge, value and support diversity of thought, opinion and approach with customers and colleagues regardless of background, culture and organizational level.
- Execute work that adheres to the City's stated principles of Diversity, Equity, and Inclusion including, but not limited to, your "duty to act" to ensure fair and equitable treatment of all persons and historically underrepresented groups.
- Fostering an inclusive and supportive environment in which everyone in the City has an opportunity to thrive.

- Incorporating an equity perspective to day-to-day work in all responsibilities, decisions and actions of providing public service.
- Effectively communicating information and ideas in writing, as well as through speech, so others will understand.
- Persuasion: Convincing others to approach things differently.
- Working independently and with minimal supervision.
- Speech recognition: Identifying and understanding the speech of another person.
- Project analysis; weighing the costs/benefits of a potential action.

License and/or Certificate:

Possession of a valid California Class C driver's license. Employees in this classification will be enrolled in the Department of Motor Vehicles (DMV) Government Employer Pull Notice Program which confirms possession of a valid driver's license and reflects driving record.

Possession of at least one of the following certifications is required:

Certification as a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Global Information Assurance Certification (GIAC), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Information Security Manager (CISM), Certified Risk and Information Systems Control (CRISC), or equivalent information security certification.

Physical Requirements and Working Conditions:
Employee accommodation(s) for physical or mental disabilities will be considered on a case-by-case basis. Positions in this class normally:

- Require vision (which may be corrected) to read small print.
- Require mobility of arms to reach and dexterity of hands to grasp and manipulate small objects.
- Perform work which is primarily sedentary.
- Is subject to the internal environmental conditions of modern and aged public buildings, facilities and physical structures and HVAC systems.
- May be required to work at a computer terminal for prolonged periods.
- May be required to work evenings and/or weekends.