THE CITY OF LOS ANGELES CIVIL SERVICE COMMISSION

CLASS SPECIFICATION

01/12/2017 CHIEF INFORMATION SECURITY OFFICER, 1404

Summary of Duties:
Under general direction from executive management, a Chief Information Security Officer (CISO) manages the design, development, implementation, operation, and maintenance of information security programs which protect information and maintenance of information, assets and technology. The CISO is responsible for protecting the confidentiality, integrity, and availability of all voice, data network, application, network infrastructure and the associated information assets; creating an accountable, information security-conscious culture through training and development; implementing and maintaining a security infrastructure based on policies and procedures; ensuring compliance with applicable Federal, State, local laws and ordinances; and fulfills equal employment opportunity responsibilities.

Class Characteristics:
The Chief Information Security Officer ensures information assets and technologies are adequately protected by providing strategic and operational information technology leadership within a department. An employee in this class exercises considerable independent judgment, initiative and management skill in overseeing and implementing information security programs. Assignments are received in as broad objectives, and work is evaluated in terms of results or goals obtained.

Distinguishing Features:
The CISO is distinguished from an Information Systems Manager in that the latter is responsible for overall planning, directing, and supervising a major functional area with complex and integrated computer systems while the former is their department's cyber security expert and is responsible for the overall information security of the department and directing/supervising cyber security personnel. The CISO develops solid working relationships with representatives from various federal and local regulatory and enforcement agencies. In addition, the CISO oversees vulnerability assessment and penetration testing (in both physical and cyber security), manages incident response and security analysis, forensics investigations, and coordinates internal and external security audits.

Both the CISCO and Information Systems Manager are bona fide supervisors and thus responsible for the performance of the full range of supervisory and management activities including the application of discipline, training, processing and resolution of grievances, and evaluation of performance.

Example of Duties:
A Chief Information Security Officer may:

- Coordinate and direct all phases of security projects from requirement definition to design, architecture, implementation, testing, support, and maintenance;

- Design, oversee, and direct the implementation of the Cyber Intrusion Command Center (CICC) and oversee the cyber security activities.
- Design the network infrastructure using security techniques to track Advanced Persistent Threat (APT), Spear Phishing, Drive-By Malware, Application Hacking and other types of cyber threats;
- Provide guidance and counsel to management working closely with division leadership teams in defining information security objectives and risk mitigation strategy;
- Implement Information Technology (IT) Business Continuity Plan using Business Impact Analysis to define the Recovery Point Objective and Recovery Time Objective of critical IT assets;
- Implement cyber security framework;
- Develop and implement security policies governing corporate security, email archiving, internet usage and access control;
- Implement internal and external vulnerability scanning to remediate the risk level of all workstations, servers, and layer 3 devices;
- Implement Enterprise Governance, Risk and Compliance to manage risks with internal controls, report compliance with regulatory requirements, and automate IT systems with security process;
- Perform or oversee staff in the performance of forensic investigations and serve as an expert witness during legal proceedings.
- Formulate, implement, and monitor a detailed program budget for all information security projects;
- Manage a team of information security professionals and ensure that subordinate supervisors meet short and long term goals, objectives, work programs, and deadlines;
- Apply appropriate managerial and supervisory skills and knowledge;
- Evaluate the operational and organizational structure of the information security division to ensure effectiveness and productivity of the available resources; and
- May occasionally be assigned to other duties to meet technological changes or emergencies.

Qualifications

Knowledge of:

- Security and privacy technologies and best practices;
- Risk and vulnerability management and remediation;
- Cyber security operations and incident management;
- Operations, services and activities of information systems security programs;
- Use of appropriate security controls and methods to reduce the risk to IT assets;
- Advanced concepts, principles and practices for IT Business Continuity Planning, Emergency Response Plan, architecture and design, voice, data network, and/or wireless security;
- Federal, State, local statutes and applicable industry regulations related to information security and privacy protection;
- Administrative and operation management knowledge including budget planning and execution;
- Supervisory principles and practices including planning, delegating, and controlling the

work of subordinate managers;

- City personnel rules, policies and procedures, and memoranda of understanding as they apply to subordinate personnel;
- Supervisory responsibility for equal employment opportunity as set forth in the City's Equal Employment Opportunity Program; and
- Techniques for motivating, counseling, and disciplining which maximizes available human resources and benefits the organization and its employees.

Ability to:

- Communicate effectively, both verbally and in writing;
- Acquire and evaluate effective network security solutions;
- Foster an innovative, collaborative, success-oriented team environment; and
- Maintain effective working relationships at all levels of the organization.

Minimum Requirements:

1. A bachelor's degree from an accredited four-year college or university; and
2. CISSP Certification (Certified Information Systems Security Professional) in good standing; and
3. Four years of full-time paid experience at the level of System Programmer III in the area of planning, designing, implementing, and configuring a secure network infrastructure and/or mission-critical applications containing enterprise data.

License: A valid California driver's license and good driving record may be required.

Physical Requirements:

Persons with disabilities may be able to perform the essential duties of this class with reasonable accommodation. Reasonable accommodation will be evaluated on an individual basis and depends, in part, on the specific requirements for the job, the limitations related to the disability and the ability of the hiring department to reasonably accommodate the limitations.

As provided in Civil Service Commission Rule 2.5 and Section 4.55 of the Administrative Code, this specification is descriptive, explanatory and not restrictive. It is not intended to declare what all of the duties and responsibilities of any position shall be.