

INFORMATION TECHNOLOGY SECURITY ADMINISTRATOR

Job Summary:

The purpose of this classification is to ensure the security operation of the City's computer systems, servers, and network connections. Employees in this classification are responsible for implementing, maintaining, and perform 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. Work is performed with limited direction and 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 position in the class. Management reserves the right to add, modify, change or rescind related duties and work assignments.)

- Supervises, organizes, plans and schedules the work of the assigned personnel who monitor, support and protect the City's technical network from cyber risks.
- Manage and performs risk and systems administration test including cyber risk management, disaster recovery, implements access control, creates and test back up procedures; validates test integrity.
- Analyze risk assessments; recommend and advice city management security enhancements; and advice city management on system security technology.
- Develops cybersecurity training and security educational awareness programs for City stakeholders on security protocols, policies, and procedures.
- Sets cybersecurity and compliance goals.
- Executes enterprise-wide policies and procedures
- Oversees staff in performing their assigned responsibilities and provides guidance as necessary.
- Interprets complex written information, develops conclusions, makes recommendations and prepares reports;
- Develop and evaluate ways to improve organizational effectiveness through evaluation of current procedures, develops conclusions and makes recommendations to improve current policy and procedures.
- May perform project management duties on assigned systems projects; maybe assigned full responsibility for specific systems and databases.
- Monitors the cybersecurity section budget and project budgets; may provide project analysis.
- 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 four (4) years of paid experience performing IT security management for a public agency; and at least two (2) years in an administrative or management capacity responsible for cyber security risk assessment, project management, and systems programs.

Option B

Master's degree in Computer Science or closely related field is highly desirable from an accredited college or university and four (3) years of paid experience performing IT security management for a public agency; and at least two (2) years in an administrative or management capacity responsible for cyber security risk assessment, project management, and systems programs. A professional cybersecurity certificate(s) is highly desirable (CISM, CISSP, GISP, AWS, etc.).

- A knowledge of Information Technology Information Library (ITIL) best practices is desirable.
- Three (3) years of paid experience managing SIEM, Vulnerability Management, and other security tools in an enterprise environment.
- Two (2) years paid Business Continuity, Disaster Recovery, and Change Management experience.

Knowledge of:

- Computers and Electronics: Electric circuit boards, processors, chips, and computer hardware and software.
- Customer Service: Principles and processes for providing customer and personal services including a desire to help customers regardless of their circumstance.
- Advanced Math: Mathematical calculations including geometry, trigonometry, algebra, statistics, and calculus.
- Computer Networks: Various hardware and software necessary to build a functional network, including routers, switches, firewalls, hubs, wiring, wireless devices, and how TCP/IP packets flow through the system.
- Programming Methodology: Necessary computer languages, basic principles, formulas, syntax, and documentation practices.

Skills and/or Ability to:

- Paying attention to detail in dealing with numbers, words, and ideas.
- Information Organization: Finding ways to structure or classify multiple pieces of information.
- Identifying problems and develop a strategic plan
- Using logic and analysis to identify the strengths and weaknesses of different approaches.
- Service Orientation: Actively looking for ways to help people.

- Analyze needs and product requirements to create a design.
- Active Learning: Working with new material or information to grasp its implications.
- Motivating, developing, and directing people as they work.
- Listening to what others are saying and asking questions as appropriate.
- Effectively communicating information and ideas in writing, as well as through speech, so others will understand.
- Persuasion: Convincing others to approach things differently.
- Conflict Resolution; Establishing and maintaining positive working relationships with those contacted in the course of work.
- Working independently and with minimal supervision.
- Applying general rules to specific problems to come up with logical answers. This involves deciding if an answer makes sense or provides a logical explanation for why a series of seemingly unrelated events occur together.
- Interactive Presentation: Effectively present information and respond to questions from groups of managers, clients, customers, and the general public.
- Speech Recognition: Identifying and understanding the speech of another person.
- Interpreting an extensive variety of technical instructions in mathematical or diagram form.
- Project analysis; weighing the relative costs / benefits of a potential action
- Discerning when important changes have occurred or likely will in a system.
- Information Technology Customer Support: Knowing and demonstrating enough hands-on customer data tools support to effectively provide additional support and lead a technical support team.

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.

Physical Requirements and Working Conditions:

Employee accommodations 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 inside environmental conditions.
- May be required to work at a computer terminal for prolonged periods.
- May be required to work evenings and/or weekends.