City of Los Angeles - Information Technology Agency

INFORMATION SYSTEMS MANAGER II

(Chief Information Security Officer)

Annual Salary: $127,347 to $158,207
(This position will be filled as exempt from Civil Service*)

DUTIES

The Information Systems Manager II will serve in the capacity of Chief Information Security Officer and will manage the operations of the Information Security division; implements comprehensive Enterprise Information Security and IT Risk Management programs to ensure the integrity, confidentiality, and availability of information; will manage a team of information security professionals; hires and trains new staff and conducts performance reviews; will manage the information security budget; works as a liaison to vendors, legal, and purchasing departments to establish mutually accepted contracts and service-level agreements; develops, maintains, and publishes up-to-date security policies, standards and guidelines, and oversees the dissemination of security policies and best practices; and implements Cyber Security Awareness training program for all employees, contractors, and approved system users.

Develops security programs that address identified risks and business requirements; implements an information security management frameworks based on Payment Card Industry (PCI) and the National Institute of Standards and Technology (NIST); provides risk guidance for IT projects including recommending technical controls; works with business units to identify and determine acceptable levels of risk; and provides periodic reporting on the current status of the information security program.

Ensures the security programs are in compliance with federal laws, regulations and policies to minimize risk and audit findings; assists the information security team with corporate compliance, audit, legal, and HR teams; serves as liaison to the IT infrastructure team to ensure the network architecture is designed with security requirements; manages security incidents to protect ITA and the City of Los Angeles' assets including intellectual property and confidential data; facilitates a metrics and reporting framework to measure the efficiency and effectiveness of the information security program.

Takes the lead role on the IT Incident Response team to respond to a disaster and recovery processes and manages security incidents to protect ITA and the City of Los Angeles' assets including intellectual property and confidential data.

This position requires specialized, scientific, and expert service in the field of information security and is unique because of the responsibilities in creating, directing, coordinating, and implementing Citywide IT security and risk management.

REQUIREMENTS

1. 5 years experience as a Chief Information Security Officer or Security Analyst; or

2. *10 years experience as a System Administrator with managing communications services which use Linux, Netware, or MS Server and advance server operating systems; or*

3. *10 years experience as a Communications Engineer with managing and configuring network routers, network management systems, intrusion detection systems, Firewalls, Application Control Engines, Proxy Servers, and anti-spam and anti-virus systems.*

* The position of Information Systems Manager II in the Information Technology Agency is an exempt, at-will management position. The incumbent will not accrue any civil service tenure, contractual employment rights or due process rights. The Information Systems Manager II is appointed by and serves at the pleasure of the General Manager. The incumbent may be removed, without any finding of cause, by the General Manager. Such removal would not be reviewable or appealable.

DESIRED QUALIFICATIONS

Extensive experience with levels of security certificates necessary to ensure integrity, confidentiality, and management of information and to take a leadership role in operating a Cyber Security Cell which includes LAPD, FBI, and Secret Service along with all key departments. One or more of the following certificates are desired:

1. **CISSP - Certified Information Systems Security Professional**
   Issuing Org.: Information Systems Security Certification Consortium (ISC)^2
   Description: "The CISSP is a certification for information security professionals and for the purpose of recognizing individuals who have distinguished themselves as an experienced, knowledgeable, and proficient information security practitioner. The CISSP certificate also provides a means of identifying those persons who subscribe to a rigorous requirement for maintaining their knowledge and proficiency in the information security profession."

2. **SSCP - Systems Security Certified Practitioner**
   Issuing Org.: (ISC)^2
   Description: "SSCP Certification was designed to recognize an international standard for practitioners of information security [IS] and understanding of a Common Body of Knowledge (CBK). It focuses on practices, roles and responsibilities as defined by experts from major IS industries. Certification can enhance an IS career and provide added credibility. Seven SSCP information systems security test domains are covered in the examination pertaining to the Common Body of Knowledge: Access Controls, Administration, Audit and Monitoring, Risk, Response and Recovery, Cryptography, Data Communications, Malicious Code/Malware

3. **CAP - Certified Authorization Professional**
   Issuing Org.: (ISC)^2
   Description: The Certified Authorization Professional (CAP) certification is an objective measure of the knowledge, skills and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Their decisions will ensure that information systems possess security commensurate with the level of exposure to potential risk, as well as damage to assets or individuals.

HOW TO APPLY

Electronic submittals are required. Interested candidates should immediately submit a resume, cover letter, three work-related references (include name, job title, affiliation, and telephone number), and responses to the supplemental questionnaire (see attachment) to:

City of Los Angeles Personnel Department
Attn: Ruben B. Vasquez
Email: hrconsolidatedrecords@lacity.org
(Note: When e-mailing your application material, the subject line should reflect your Name and the Job Title you are applying for.)
Questions may be referred to Ruben B. Vasquez at (213) 978-3390

The filing period may close on Friday, July 11, 2014, by 4 p.m.
or until sufficient resumes are received.

The City of Los Angeles is an Equal Employment Opportunity Employer

CHIEF INFORMATION SECURITY OFFICER (ISM II)
SUPPLEMENTAL QUESTIONNAIRE

1. Please describe your experience in developing and implementing a comprehensive security program for a large-scale organization (e.g., 20,000 employees or more)

2. Please describe your experience in developing security policies, standards and procedures and include the size of the organization where these were developed and implemented.

3. Describe the steps to build a security operations center and what tools and process would take place in that environment.

4. Please describe your experience in conducting a risk assessment (RA). What initiated the RA need, what was the size of your team, what was your role and what were the results of the RA?

5. Please describe your experience with forensics and eDiscovery.

6. Please list your current professional licenses and certifications applicable to information.

7. . Describe the importance of a SIEM Tool and what it does for an organization.