Compensation and Benefits

Annual Salary: $132,079 - $199,912 (MAPP Range R14 – effective 10/1/2017)

The appointee will receive an annual salary, commensurate with qualifications and earning history, as well as an excellent program of benefits that allows employees to choose the benefits that meet their specific needs.

The package includes:

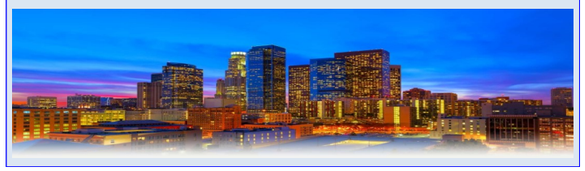
- Retirement Plan – New appointees will participate in a contributory defined benefit plan.
- Cafeteria Benefit Plan – The County funds its cafeteria plan using a tax-free contribution of an additional 14.5% to 17% of the employee's monthly salary.
- Flexible Spending Accounts – In addition to tax-fee medical and dependent care spending accounts, the County contributes $75 per month to an employee's dependent care spending account.
- Savings Plan (401k) – Optional tax-deferred income plan that may include a County matching contribution up to 4% of employee's salary.
- Deferred Compensation Plan (457) – Optional tax-deferred income plan that may include a County matching contribution up to 4% of employee's salary.
- Holidays – 12 paid days per year.

SOCIAL SECURITY ACT OF 2004 Section 419(c) of Public Law 108-203, the Social Security Protection Act of 2004, requires State and local government employers to disclose the effect of the Windfall Elimination Provision and the Government Pension Offset Provision to employees hired on or after January 1, 2005, in jobs not covered by Social Security. The County of Los Angeles does not participate in the Social Security System. All newly hired County of Los Angeles employees must sign a statement (Form SSA-1945) prior to the start of employment indicating that they are aware of a possible reduction in their future Social Security benefit entitlement. For more information on Social Security and about each provision, you may visit the website at www.socialsecuity.gov, or call toll free (800) 772-1213.

Persons who are deaf or hard of hearing may call the TTY number (800) 325-0778 or contact a local Social Security office.

This announcement may be downloaded from the

COUNTY OF LOS ANGELES website at:
http://hr.lacounty.gov.



Selection Process

Each candidate's background will be evaluated on the basis of information submitted at the time of application to determine the level and scope of the candidate's preparation for this position. The resume should include any additional information that the candidate wishes considered. Only the most qualified candidates, as determined by the screening process, will be invited to participate in the selection process. The names of the most highly qualified candidates will be submitted to the Chief Information Officer for final selection.

NOTE: A background investigation will be completed on the candidate selected for this position.

Filing Instructions

Highly qualified candidates are invited to submit a statement of interest, a comprehensive resume detailing their knowledge, skills, and abilities relevant to this position and current salary information. Submission should include **ALL** of the following:

- Candidate's ability to meet the requirements as stated in the Qualifying Education and Experience and Desirable Qualifications sections of this recruitment announcement.
- For organizations and programs managed, the name of each employer, job title, size of organization's budget, number and composition of personnel supervised, scope of management responsibilities, functions managed, dates of employment, and current salary.
- Names of schools, colleges and universities attended, dates attended, degrees earned, and field(s) of study. Please enclose verification of degree(s), licenses and certificates together with the resume.

Materials received by October 2, 2017, will be given first consideration. Electronic submittals are strongly preferred and should be submitted to:
CEOExecRecruitment@ceo.lacounty.gov
Please indicate the position title of Chief Information Security Officer (UC)

in the subject line of your e-mail

Hardcopy submittals by mail or hand delivery should be addressed to:
Stacey M. Winters
County of Los Angeles Chief Executive Office
500 West Temple Street, Room 785
Los Angeles, CA 90012

You may also fax your application to:
Stacey M. Winters at (213) 613-0744

Confidential inquiries welcomed to :
Stacey M. Winters
Email: swinters@ceo.lacounty.gov
Telephone (213) 974-2617

The County of Los Angeles

Invites Resumes for

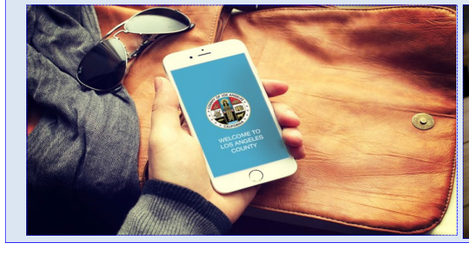
CHIEF INFORMATION SECURITY OFFICER

(UNCLASSIFIED)

Open from September 18, 2017 - until filled

Annual salary: $132,079 – $199,912

(Published Salary Effective October 1, 2017)



County of Los Angeles

The County of Los Angeles, listed in Forbes Magazine as one of America's Best Employers for 2015, 2016 and 2017, is the largest employer in Southern California with more than 109,000 employees in over 34 departments. The county provides vital, wide-ranging services to a diverse population of 10 million residents.

The County has more residents than any county in the nation, and within its boundaries are 88 cites. It is rich in cultural diversity and home to world-renowned museums, theaters, the nation's motion picture industry, major universities, and numerous five-star restaurants.

The County is governed by a five-member Board of Supervisors who are elected on a nonpartisan basis and serve four-year terms. As the governing body, the Board of Supervisors serves as both the executive and legislative authority of the largest and most complex county government in the United States.

The County's annual budget for fiscal year 2017-18 is over $30 billion, with funding for approximately 109,000 positions across over 34 departments to serve the County's residents and its diverse population.

The Chief Executive Office

In its role as the central executive, strategic, and administrative agency for the County, the Chief Executive Office (CEO) is responsible for a wide range of activities, including managing and directing budget and operations, employee relations, compensation, asset management, strategic integration, legislative affairs, intergovernmental relations, risk management, strategic planning, and Countywide communications.

The Chief Information Office (CIO) resides in the Strategic Integration Branch of the CEO. Within the CIO, the Information Security Office establishes and publishes countywide information security policies and standards to mitigate risks to computer assets and data and directs the enterprise information security program.

The Position

The Chief Information Security Officer (CISO) reports to the County's Chief Information Officer and is responsible for coordinating information and providing executive leadership to integrate Countywide security and privacy-related programs designed to protect all County IT systems and data, through subordinate CIO staff and through department designated Information Security Officers. This position requires extensive, up-to-date technical knowledge in information systems, detailed knowledge of security and privacy technologies and best practices, and the use of appropriate security controls and methods. The CISO must possess an extensive knowledge of IT security, privacy legislation and related policy issues; and the ability to develop and maintain effective interpersonal relationships with internal and external managers, IT technical staff, legal staff and related industry experts. The CISO represents the County's interests before State and federal agencies and regulatory bodies. The CISO serves as the official Health Insurance Portability and Accountability (HIPAA) Information Security Officer for the County, and coordinates and oversees all HIPAA security for the County.

Although most of the major administrative units and departments manage and operate their internal IT environments, the CISO is responsible for working collaboratively with those departments to ensure security governance and regulatory compliance, policy development and management, and security training and awareness development. The CISO directs countywide security initiatives and team to manage and mitigate information security threats.

Qualifying Education & Experience

TRAINING AND EXPERIENCE

A Bachelor's Degree from an accredited college or university in Computer Science, Information Systems, Public or Business Administration, or a related field, **AND:**

OPTION A: A minimum of two years of experience at the level of the County of Los Angeles classes of Departmental Information Security Officer II or Information Technology Specialist, responsible for developing, implementing or monitoring a large and complex information systems security program for a diverse multi-service public sector organization. **-OR-**

OPTION B: Five years of management experience in the information technology profession, three years of which must have been concentrated in information security. This must include managing a security program for a large public or private sector organization.

LICENSE: A valid California Class C Driver License or the ability to utilize an alternative method of transportation when needed to carry out job-related essential functions.

PHYSICAL CLASS: 2 – Light.

Desirable Qualifications

- Possession of a current Certified Information Systems Security Professional (CISSP) certification issued by the International Information Systems Security Consortium, or other related security accreditation/certification.
- Demonstrated knowledge and experience in IT planning, auditing, and risk management, as well as contract and vendor negotiation in the IT field.
- Demonstrated working knowledge of government regulations and laws related to privacy and security.
- Experience with risk and control assessment of information assets.
- Experience in managing threat and vulnerability assessments of information assets, including developing and initiating of preventative measures.
- Demonstrated knowledge of identity and access management practices and technology.
- Excellent oral and written communication skills with an ability to adapt approach, language and style to different audiences.
- Demonstrated ability to serve as an effective member of the leadership team and communicate information security-related concepts to a broad range of technical and non-technical employees.
- Demonstrated collaboration and team-building skills and the ability to build consensus around challenging topics.

Examples of Key Duties

The Chief Information Security Officer's duties include, but are not limited to the following:

- Oversees the development and implementation of Countywide IT security policies and procedures to protect the County from internal and external IT threats and vulnerabilities.
- Represents the Chief Information Officer with County departments, information technology advisory bodies, and other committees or agencies involving County policies, plans, methodologies and programs related to security, privacy and confidentiality of data and information technology assets.
- Directs the preparation of short and long term strategies for optimizing the County's Information Security Plan; and formulates and recommends Countywide policies for detecting, deterring and mitigating information security threats.
- 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.
- Directs the handling of IT security breaches and related incidents, including overseeing the activation of the County Computer Emergency Response Team (CCERT) or other incident response teams.
- Coordinates resource-sharing between departments to mitigate IT security incidents and IT security related notifications to the Board of Supervisors.
- Serves as a subject matter expert and internal consultant on the data security implications of proposed new major information technology projects and programs, and makes recommendations to the Chief Executive Officer and affected departments.
- Reviews and recommends the professional development curriculum for County IT security and privacy staff to ensure adequate and appropriate training standards in IT security and protection measures, and coordinates related training and awareness programs.
- Directs the development and promotion of security and privacy awareness training and education for all levels of the County organization structure on an ongoing basis.
- Participates in the development and implementation of disaster recovery and business continuity plans to ensure that appropriate IT security measures are addressed.
- Participates in the development, implementation and compliance-monitoring of IT security agreements, business associate agreements, chain-of-trust agreements, and Memoranda of Understanding (MOUs) that involve access to or exchange of County information, to ensure all security concerns are addressed.
- Maintains current applicable federal and state IT security laws and standards data to facilitate County adaptation and compliance.