COMPENSATION & BENEFITS

ANNUAL SALARY: $145,815 - $226,772

The unclassified appointee will receive an annual salary, commensurate with demonstrated qualifications, 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 provides a tax-free contribution of 14.5% to 17% of the employee's monthly salary from which to purchase health insurance and other benefits.
- **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.

HOW TO APPLY

This unclassified position is open to from **September 2, 2021** until filled.

First consideration will be given to applications received before **September 16, 2021**.

Please go to https://bit.ly/3gUKCmI and submit your application, letter of interest, CV, and verification of degrees.

For confidential inquiries, please contact:

Alice Ting
Executive Recruiter
Talent Acquisition Division
Department of Human Resources
(323) 400-9014
ating@hr.lacounty.gov

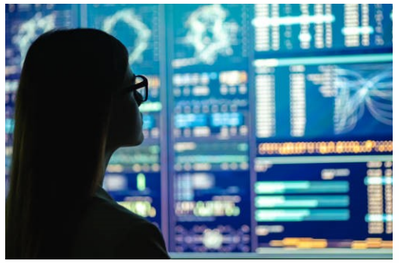
Los Angeles County
DEPARTMENT OF
Human Resources

The County of Los Angeles Chief Executive Office Invites Resumes for:

CHIEF INFORMATION SECURITY OFFICER (UNCLASSIFIED)

Open for applications starting September 2, 2021.

To enrich lives through effective & caring service.



THE COUNTY

As the largest employer in Southern California, the County of Los Angeles has over 110,000 employees in 37 departments and an operating budget of over $36.5 billion. The County provides vital and wide-ranging public services to a diverse population of 10 million residents.

With 88 cities and more than 120 unincorporated areas, the County is proud of our vast multicultural populations, which speak more than 220 languages. We endeavor to hire persons who understand and represent the various communities within our County.

THE CHIEF EXECUTIVE OFFICE

The Chief Executive Office (CEO) is the central executive, strategic, and administrative agency driving transformative change to improve the lives of our diverse constituents. We lead collective efforts with other departments to achieve priorities established by our Board regarding affordable housing, sustainability, economic development, healthcare integration, homelessness, child protection, justice reform, anti-racism, diversity and inclusion, and poverty. As the administrative agency responsible for the County's $36.5 billion budget, we handle specialized functions to lead and maximize the use of County assets; advocate the County's position on State and federal agendas; lead and implement the Countywide Strategic Plan; implement risk management strategies to mitigate financial loss; and convey the County's message through a variety of communication platforms.

THE OPPORTUNITY

The CEO of Los Angeles County is seeking well qualified candidates with a successful track record of leading security strategies for large complex organizations to serve as the new **Chief Information Security Officer (CISO)**. This unclassified position reports to the County's Chief Information Officer and is responsible for coordinating information and providing executive leadership to integrate Countywide security related programs designed to protect all County IT systems and data, through subordinate CIO staff and department designated Information Security Officers. This position requires extensive, up-to-date technical knowledge in information systems, detailed knowledge of security technologies and best practices, and the use of appropriate security controls and methods. The CISO must possess an extensive knowledge of IT security and related policy issues; and the ability to develop and maintain effective interpersonal relationships with internal and external managers, IT technical staff, legal and privacy staff and related industry experts. The CISO represents the County's interests before State and federal agencies and regulatory bodies and serves as the official Health Insurance Portability and Accountability (HIPAA) Information Security Officer 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 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's license or the ability to utilize an alternative method of transportation when needed to carry out job-related essential functions .

DESIRABLE QUALIFICATIONS

- A current Certified Information Systems Security Professional (CISSP) certification issued by the International Information Systems Security Consortium, Certified Information Security Manager issued by the Information Systems Audit and Control Association or other comparable 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 information security.
- 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.

ESSENTIAL DUTIES

- Develop and maintain the County's Information Security Program including policies, standards, and procedures; cybersecurity control evaluation, selection, and implementation; and architectures, products and services, pursuant to County Chief Information Office (CIO) architectures, standards and guidelines, and Board polices and applicable laws.
- Oversee the development and implementation of Countywide IT security policies and procedures to protect the County from internal and external IT threats and vulnerabilities.
- Represent the CIO with County departments, IT advisory bodies, and other committees or agencies involving County policies, plans, methodologies and programs related to security.
- Direct the preparation of short- and long-term strategies for optimizing the County's Information Security Plans.
- Direct and participate in the identification of security risks, development and implementation of security management practices, and the measurement and monitoring of security protection measures.
- Direct the handling of IT security breaches and related incidents, including overseeing the activation of the County Cyber Incident Response Committee (CCIRC) or other incident response teams. Coordinate resource-sharing between departments to mitigate IT security incidents and IT security related notifications to the Board of Supervisors.
- Serve as a subject matter expert and internal consultant on the information security implications of proposed new major information technology projects and programs and make recommendations to the Chief Executive Officer and affected departments.
- Direct the development and promotion of security awareness training for all levels of the County organization structure.
- Participate in the development and implementation of disaster recovery and business continuity plans to ensure that appropriate IT security measures are addressed.
- Participate 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.