The Los Angeles County Office of Education is dedicated to equal employment opportunity and fosters a workforce that embraces and reflects the rich diversity of Los Angeles County.

Information Systems Security Officer

$7793 to $9654 Monthly

Insurance:
Paid premiums for your choice of several medical, dental, vision, and life insurance plans
To learn more, visit: www.lacoe.edu

Online applications must be submitted by:
Open Until Filled
(Apply ASAP)

Retirement:
Defined Benefit, Public Employee’s Retirement System (PERS), 2.5% @ 55

Paid Time Off:
24 days vacation.
14 holidays. 12 illness days.

Los Angeles County Office of Education (LACOE) is conducting a national search for highly motivated candidates for the position of Information Systems Security Officer. This is a unique opportunity for an accomplished systems security professional to develop and implement an ongoing risk assessment program and information security management system for the nation’s largest regional education agency.

The Position of Information Systems Security Officer
The Information Systems Security Officer will report directly to the Chief Technology Officer and will be responsible for planning, developing, and maintaining a comprehensive, enterprise-wide information security program to protect LACOE electronic data and network infrastructure from external and internal security breaches and to ensure that security measures taken are in compliance with statutory and regulatory requirements regarding information access, security and privacy.

LACOE Technology Services
LACOE’s Technology Services provides technology infrastructure development and support, network services, software/web application development, instructional technology outreach to teachers and administrators and database administration to LACOE operating divisions and over 70 local school districts.

Areas of support include project management, technical analysis and consulting, system design, application development, stress testing, data backup, and disaster recovery planning. In addition, network services include an Internet Service Provider for over 65 school districts, content filtering, secure network access to LACOE business applications, and access to the California K-12 High Speed Network. Technology Services provides customized multimedia services including video streaming, interactive CD-ROM and DVD production, website development, videoconferencing, studio and remote video production. For its customers, these services translate into improvements in business operations, classroom support, student instruction, and staff training.

Technology Services strengthens LACOE’s position as a leader and innovator in the fields of educational computing and telecommunications services, and gives technology-related issues higher visibility throughout the organization. Technology Services provides expertise in mainframe and server-based payroll, human resource, and financial applications. Instructional technology outreach assists and trains educators countywide on how to integrate technology into teaching and learning and helps align specific curricula to California’s K-12 content standards. Technology Services provides LACOE and the Los Angeles County educational community with a broad range of state-of-the-art solutions, organized among the various Technology Services divisions.
The Well-Qualified Candidate
The well-qualified candidate will have a solid record of accomplishment in implementing strategies and managing systems in information systems security. The well-qualified candidate...

has the knowledge of:

- Broad information security issues, requirements and trends
- Compliance requirements or standards related to Federal Rules of Civil Procedure (FRCP), e-Discovery, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Children’s Internet Protection Act (CIPA), Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST), Sarbanes-Oxley and other information security related laws and regulations
- Risk assessment methods and techniques
- Security software and tools
- Auditing standards and techniques
- Application architecture and design, development environments, database design and normalization, network security and infrastructure
- Authentication, authorization and encryption technologies
- Forensic techniques for investigating incidents
- Implementation of data security strategies for large mainframe or data center environments

has the ability to:

- Identify problems, collect data, establish facts, draw valid conclusions, and generate a range of alternative solutions and courses of action
- Enable constructive and productive group interaction and maintain group commitment to goals and objectives
- Provide accurate, clear, and timely information using multiple communications media
- Effectively manage multiple projects
- Prioritize and plan work activities
- Identify and apply new developments in information security technology
- Act as a change agent to facilitate improvement in information security
- Maintain confidentiality of sensitive information
- Establish and maintain effective working relationships in cross-functional teams that include both technical and non-technical members
- Communicate effectively, both orally and in writing

preferably possesses one or more industry certifications, such as:

- Certified Information Systems Security Professional (CISSP)
- Cisco Certified Network Associate Security (CCNA Security)
- Systems Security Certified Practitioner (SSCP)
- Microsoft Certified Systems Engineer (MCSE) with specialization in Security

For a complete job description go to www.personnelcommission.com
Required Education and Experience  (must be met at time of application)

**Education:** A bachelor's degree in computer science, business administration, or a closely related field, from an institution of higher learning accredited by a regional accrediting organization recognized by the Council of Higher Education Accreditation. Professional certification such as Certified Information Systems Security Professional (CISSP) or equivalent is desirable.

**Experience:** Five years of experience in managing information and system security in complex multi-vendor and multi-platform computer systems and network environments.

**Notes:** A valid California driver's license and the availability of private transportation or the ability to provide transportation between job sites is required.

Selection Process

Candidates who meet the minimum requirements above, will be invited to participate in an examination consisting of a training and experience review, a performance examination and an oral technical interview.

For additional information on our selection procedures please visit Exam Preparation on our website. Selection and promotion are based on a competitive examination process. Candidates who pass all exam parts are ranked according to overall exam score and placed on an eligibility (hiring) list. Vacant positions are filled from the top three ranks. Eligibility lasts for 12 months; however, additional recruitment may occur under a separate bulletin with additional candidates being merged onto the eligibility list. Some positions that involve public contact may require bilingual proficiency for which selective certification may apply (Education Code 45277.5). In addition, the eligibility list resulting from this examination may be used to fill vacancies in related job classifications for which no eligibility list exists (Education Code 45272). Veterans' Credit may be awarded for entry jobs.

Reasonable accommodations in completing an application and testing are available to individuals with disabilities. If you would like to request an accommodation, please call (562) 803-8360 as early as possible.

To apply, click on the “Apply” link at the top of this page.

1) Create a User ID and password if you haven’t already done so.  2) Log in.  3) Create or update your MASTER PROFILE.  4) Complete the QUESTIONNAIRE.  5) Submit the application.

Resumes are not accepted in place of a completed application nor will they be reviewed as part of the examination process. Diploma and degree verification (including equivalency of foreign degrees) must be submitted in the form of unofficial transcripts or a copy of your diploma. This documentation may be scanned and included with your online application or brought at the last examination part.

Complete applications for this job must be submitted before the end of the announced deadline date unless an extended deadline is shown on the website for this opportunity.

LACOE Personnel Commission, 9300 Imperial Hwy, EC-Annex, Downey, CA 90242
Phone: 562.803.8360 -- Contact: Liane Kwan -- (M-F 8:00am–5:00pm)
For complete application information, please go to www.personnelcommission.com

This examination is authorized as Open to the Public.
Recruitment ID: 11-414

This announcement does not constitute an implied contract.  Any part of this announcement is subject to change.
1. Please list all current information systems security certifications you have earned and their expiration dates. Include in your description the certification subject matters, certification requirements, and recertification requirements. Please also attach copies of your security certificates with your application.

2. Describe your experience in developing and implementing an ongoing risk assessment program and information security management system targeting electronic information and infrastructure security. Please include the steps you took to assess the security risk and the security measures that you implemented for security breach prevention, detection and remediation. Please attach documented examples with your application.

3. Please describe your experience in planning, implementing and monitoring data security and disaster recovery specifically for mainframe and open system architectures. Please attach documented examples with your application.

4. Please describe any significant accomplishments you have had in technology acquisition, implementation, and revisions to improve information systems security.

5. Describe your experience in providing organization-wide consultation and advice on data security management, disaster recovery, and emergency preparedness planning.