Information Systems Security Officer

Class Code:
9062

Bargaining Unit: Unrepresented - Management

SUPERIOR COURT OF CALIFORNIA, COUNTY OF ALAMEDA
Established Date: December 18, 2025

SALARY RANGE

SEE SALARY SCHEDULE

JOB DESCRIPTION:

JOB DEFINITION
Under direction, the Information Systems Security Officer (ISSO) develops and manages the Court's Information Technology (IT) Security program; Works closely with IT teams to identify, assess, and mitigate security risks; works with incident response management teams to contain security incidents and prevent future incidents; leads the implementation of risk mitigation efforts, performs monitoring and testing, and assesses the output of tests and scans to develop corrective action plans, and recommends policies and procedures to senior leadership; and performs other related duties as assigned.

DISTINGUISHING FEATURES
The ISSO is a management-level class that reports to the Information Technology Director within the Office of Information Technology. The ISSO should have a forward-looking approach to IT security, risk mitigation, and resilience, to ensure all technological infrastructures reflect best-in-class security practices. The ISSO is distinguished from the Sr. IT Manager in that the latter is responsible for planning, coordinating, and supervising complex operations and work of professional staff within multiple information technology work units of Application Services and IT Business Solutions or Infrastructure Services and Client Services and provides guidance and direction to other IT Managers; whereas, the former is a very specialized position that manages IT Security, including safeguarding infrastructure and managing vulnerabilities to enforcing best-in-class cybersecurity practices, compliance and risk mitigations.

EXAMPLES OF DUTIES:

1. Analyzes networks, systems, hardware, and software for security vulnerabilities, and designs and configures security measures.

2. Manages court-wide information security awareness and training programs.

3. Configures and uses tools, industry best practices and security framework guidelines such as National Institute of Standards and Technology to monitor and investigate computer networks for security issues and suspicious activities; prepares security incident reports.

4. Researches emerging threats and vulnerabilities to aid the identification of network incidents, and creates new architectures, policies, standards, and guidance to address them.

5. Creates business continuity/disaster recovery plans; publishes test results and implements changes to address deficiencies.

6. Coordinates the testing of new computers, software, and networking hardware before implementation to safeguard and secure the court's information systems.

7. Assesses the vulnerability of the Court's information system; develops and executes the Court's information security strategies, policies, and procedures, including the identification and analysis of information security threats in order to protect the Court's computer infrastructure, network, and data. Creates systems and procedures to assess and track compliance with Court security policies.

8. Coordinates with vendors, participates in or leads cross functional project teams, and perform critical incident response.

9. Meets and consults with customers and vendors regarding IT security needs; oversees and participates in the design, development, delivery and/or implementation of IT security-related products to meet those needs; assumes responsibility for procurement of services and goods required.

10. Responsible for the development of specifications for "requests for proposal" pertaining to external security-related services; reviews submissions and provides recommendations on vendor selection; ensures vendor performance meets compliance, Court standards and specification.

11. Directs the management and governance of security-related projects of varying size and scope to enhance and/or upgrade technology services and utilization.

12. Prepares reports, correspondence and other documents; participates on committees and task forces; attends meetings, conferences and training sessions.

13. May supervise or lead other IT security related professionals, including overseeing their work quality, training, instruction, and work assignments.

14. Performs other related duties as assigned.

MINIMUM QUALIFICATIONS:

Education:

Possession of a Bachelor's degree from an accredited college or university with major coursework in computer science, information technology security, or a closely related field. Possession of one or more approved information technology certificates and/or completion of other approved IT security-related training may substitute for some or all of the required education.

Experience:
Four (4) years of experience in a Cybersecurity/IT Security environment with responsibility for supervising/directing programs and staff in IT Security.

Desired Qualifications:

License or Certifications are preferred, though not required:

- Preferred: CISSP, CISM, CompTIA Security+, CySA+, CISA
- Nice to have: Cisco CCIE, VMWare, Microsoft Certified Expert

KNOWLEDGE AND ABILITIES:

Knowledge Of: Methods, tools, and procedures, including development of IT security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services; Architecture and typology of software, hardware, and networks, including LANs, WANs, Firewalls, VPNs, Telephony and telecommunication systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software; Operating system architecture, characteristics, capabilities, constraints, and commands applicable to the Court's information systems environment; One or more scripting languages (e.g. Perl, Python and PowerShell); Principles, methods, and tools of quality assurance, quality control, and reliability used to ensure that a project, system, or product fulfills requirements and standards. Policies, procedures, laws, and regulations applicable to assigned responsibilities including internal and external security audits; Public cloud, government cloud, secure hybrid or multi-cloud and on-prem; Virtual infrastructure architecture and design principles; Best practices and methods of cybersecurity administration, governance and policy creation; Principles and practices of customer service, telephone etiquette, sound business communication; Basic practices and procedures of budgeting and purchasing.

Ability to: Perform complex cybersecurity network and systems administration functions; Troubleshoot and resolve complex security threat vectors, attacks, patterns, and remediation; Write and verbally communicate in a professional manner, communicate with leadership; Exercise sound judgment within specific cybersecurity policy guidelines and laws; Keep technical skills current to meet continuing cybersecurity responsibilities; Understand and respect limits of authority; Maintain confidentiality of Court documents and records; Deliver high-quality IT security products, processes and solutions in a timely and efficient manner; Coordinate and administer a variety of information technology projects; Gather and evaluate information in order to reason logically, draw valid conclusions, take appropriate actions and/or make appropriate recommendations; Develop information technology designs, flow charts, report layouts and screen designs; Communicate technical information to a wide variety of users; Interpret and apply complex and technical information pertaining to computer and network systems; Adapt quickly to changes in policies, procedures, assignments and work locations; Communicate effectively, both verbally and in writing; Establish and maintain effective working relationships with those encountered during the course of the work.

WORKING CONDITIONS

Work is typically performed in an indoor office environment, but occasionally requires travel to other locations. Work environments may occasionally be noisy. Occasional evening, holiday and/or weekend work may be required.