Position Overview

Position Overview

Supervisory Organization Information Security Office (Robert Leon)

Organization Assignments Company: Covered California
Cost Center: 4201000401 INFORMATION TECHNOLOGY DIV COST CENTER

Effective Job Requisitions JR-100795 Section, Information Security - Section (Open)

Job Posting Title Section, Information Security - Section

Job Description Summary Under the general direction of the Chief Information Security Officer, Information Technology Manager II, the Information Technology Manager I, Information Security Manager, manages, oversees, and operates the Covered California's Information Security Program. Ensures the protection of the agency’s information assets and compliance with federal and state information security mandates, policies, standards, and procedures. Provides expert guidance and consultation on complex, technical information security issues and projects. This position serves under the Information Security Engineering domain. Duties may include access to information systems containing protected enrollee information, including federal tax information, protected health information, and personally identifying information.

Job Description

Job Description

35% (E)

Information Security Operations: Oversees the management and operation of various security tools such as firewalls, intrusion prevention/detection systems, web application firewalls, web content filtering, network access control systems, Security Information and Event Monitoring (SIEM), Managed Security Service Provider (MSSP), and endpoint security solutions. Leads the Information Security Incident Response Plan team and manages the coordination efforts of technical security assessments and audits of key security controls for both internally and externally facing systems/resources to ensure compliance with applicable state and federal laws, regulations, and agency policies including CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E). Provides technical leadership and guidance to departmental staff on appropriate responses to risk assessment findings. Oversees the findings from security audits and assessment work and provides improvement options and recommendations to management. Contributes to the coordination of the identification, ownership, and classification for all systems, records, files, and databases to ensure the confidentiality, integrity and availability of agency information assets. Ensures proper implementation of security tools to assess systems and assets. Oversees the vulnerability management program efforts for the enterprise to ensure vulnerabilities that pose significant levels of risk are prioritized and address in a timely manner. Contributes to the development and implementation of information security policies, standards, procedures, and guidelines. Oversees the creation of secure configuration standards for hardware, software, and network devices. Maintains the Plan of Action Milestones (POAM), Risk Management and Privacy Compliance, and Technology Recovery Plan and ensures timely submission to control agencies as required. Reports on IT security trends and best practices to maintain operational readiness and preparation for future operational needs utilizing input from staff, clients, peers, and independent research. Conducts research and performs analysis of products or services to inform enterprise IT decisions. Develops written summaries or other materials to present findings. Develops, documents and maintains documentation for new and existing process and procedures including any training or reference materials to support implementation. Contributes in the development of technical road maps, enterprise architecture standards, and strategies to best align technology solutions with business and organizational needs while maintaining compliance. Ensures that assigned contracts and agreements are administered and managed in accordance with the applicable policies and procedures of the agency, the State Contracting Manual and the California Government Code.

35% (E)

IT Program: Manages ongoing agency compliance with IT policy requirements across the enterprise. Develops emails, newsletters, and other communications for department staff to promote awareness and education of Information Security initiatives and trends. Creates and maintains on-line repositories of IT and Information Security information that can be accessed by users (e.g., user guides or other reference material). Collaborates and works across the various functions of the IT Division, including providing direct user support, to resolve issues.

Develops and maintains knowledge of systems and tools within the IT Division and performs ad hoc functions on an as-needed basis. Responds to calls, emails and in-person inquiries to resolve end user issues or questions related to the use of IT systems, processes, or security incidents. Oversees and tracks Information Security and network license agreements and renewals. Oversees training and support of user testing of IT initiatives.

20% (E)

Administrative and Management: Monitors and tracks the progress of tasks as directed by IT Leadership. Follows up with task owners to update status. Collects and monitors metrics/data, conducts analysis, and produce reports to support Information Security operations. Provides direction, guidance, and leadership to subordinate staff, or contracted personnel in implementing and maintaining enterprise and security services. Fosters an environment of teamwork and collaboration and recognizes and communicates individual and team accomplishments. Identifies and documents performance or conformance issues, develop improvement plans, provide opportunities for continuous learning. Contributes to workforce planning, budgeting, and succession planning.

10% (M)

Miscellaneous Duties: Maintains up to date knowledge about state policies and processes and industry best practices related to information security and network administration. Invests in personal development through continuous education to maintain position-related knowledge. Collaborates with leadership and cross-functional teams to develop solutions for complex problems. Leverages expertise in complex information systems to effectively communicate complicated and technical concepts or issues clearly and articulately through non-technical means. Participates in the development of the agency’s Technology Recovery Plan, Business Continuity Plan, Software Management Plan, and other planning efforts. Travels statewide to attend meetings, trainings, and seminars.

Scope and Impact

The incumbent reports to the Chief Information Security Officer, and the responsibility for decisions and consequence of error is significant as the incumbent provides critical services to carry out department operations and ensure new initiatives and projects are properly scoped, requirements are clearly documented, schedules and budgets are in place, the efforts are appropriately resourced, and project management plans, quality plans, and communication plans are developed, reviewed, and accepted by sponsors and key stakeholders. Repercussions of potential failures or errors would result in missed deadlines, security and privacy breaches, system downtime, and could be catastrophic to the Exchange/CC and its consumers.

Physical and Environmental Demands

WORK ENVIRONMENT

Work in a climate-controlled, open office environment, under artificial lighting; exposure to computer screens and other basic office equipment; work in a high-pressure fast-paced environment, under time critical deadlines; work strenuous and long hours; must be flexible to work days/nights, weekends and select holidays as needed; during peak enrollment periods, may be required to work overtime; appropriate dress for the office environment.

ESSENTIAL PHYSICAL CHARACTERISTICS

The physical characteristics described here represent those that must be met by an employee to successfully perform the essential functions of this classification. Reasonable accommodations may be made to enable an individual with a qualified disability to perform the essential functions of the job, on a case-by-case basis. Ability to attend work as scheduled and on a regular basis and be available to work outside the normal workday when required. Continuous: Upward and downward flexion of the neck. Frequent: sitting for long periods of time (up to

70%); repetitive use of hands, forearms, and fingers to operate computers, mouse, and dual computer monitors, printers, and copiers (up to 70%); long periods of time at desk using a keyboard, manual dexterity and sustained periods of mental activity are need; using headsets to talk with internal and external customers for extended periods (up to 60%); Frequent: walking, standing, bending and twisting of neck, bending and twisting of waist, squatting, simple grasping, reaching above and below shoulder level, and lifting and carrying of files, and binders.

Working Conditions and Requirements

a. Schedule: 8 hours per day/ 40 hours per week. The incumbent may be required to work outside of standard business hours to support 24/7 service requests.
b. Travel: Travel maybe required up to 5% travel between Exchange/CC locations, other state departments and various locations.
c. Other: May require rotating 24x7 on-call support responsibility as well as weekend, and holiday support. Incumbent is required to carry a department issued cellular telephone.

Available For Hire	Yes
Hiring Freeze	No