

Duty Statement
Department of Managed Health Care

OFFICE: Office of Technology and Innovation	EFFECTIVE DATE:
CLASSIFICATION: Information Technology Specialist II	DATE APPROVED: 06/21/2024
POSITION: 521-1414-xxx	TELEWORK DESIGNATION: <i>Remote-Centered</i>
WORKING TITLE: Application Development Security Operations Engineer	

DEPARTMENT OBJECTIVE:

The mission of the California Department of Managed Health Care (DMHC) is to protect consumers’ health care rights and ensure a stable health care delivery system. The DMHC accomplishes its mission by ensuring the health care system works for consumers. The Department protects the health care rights of more than 29.7 million Californians by regulating health care service plans, assisting consumers through a consumer Help Center, educating consumers on their rights and responsibilities and preserving the financial stability of the managed health care system.

PROGRAM OBJECTIVE:

The Office of Technology and Innovation (OTI) enables the DMHC to deliver essential services to the State of California using information technology. The systems that the OTI supports have become a valuable tool in the execution of DMHC’s business functions. The Information Security Office (ISO) develops, reviews, and maintains programs associated with the protection of assets that includes personnel, information, software and hardware. The ISO is responsible for the ongoing application of principles, policies and procedures to maintain, monitor, control and protect cyber infrastructure in order to ensure the confidentiality, integrity and availability of production systems and applications.

GENERAL DESCRIPTION:

Under direction of the IT Manager I as part of the Information Security Office (ISO), the incumbent works both independently and as part of the Information Security team in support of the mission of the department through continuous improvement of the department’s information security program and dedication to protecting the confidentiality, security, and availability of department information resources. Areas of responsibility include cloud and on-premises information security technology systems and services, information security operations and incident response, information security audits and assessments, information security policy and procedure, and information security compliance and reporting.

IT DOMAINS

- | | |
|--|--|
| <input type="checkbox"/> Business Technology Management | <input type="checkbox"/> IT Project Management |
| <input checked="" type="checkbox"/> Client Services | <input checked="" type="checkbox"/> Information Security Engineering |
| <input checked="" type="checkbox"/> Software Engineering | <input checked="" type="checkbox"/> Systems Engineering |

TYPICAL DUTIES:

Employee must be able to perform the following duties with or without reasonable accommodation.

<u>PERCENTAGE</u>	<u>JOB DESCRIPTION</u>
--------------------------	-------------------------------

Essential (E)/Marginal (M)

40% (E)

Application Security Program

Establish, document, and maintain an Application Security program. Combine vulnerability detection via web scans, application tools, and threat mitigation to create a resolution plan.

Consult developers on questions related to vulnerability reports to include explaining vulnerabilities and significance, circumstances which an issue may be exploitable, and providing suggestions on how an issue may be remediated.

Assist in application security testing, security requirements, and helping integrate security into the Software Development Lifecycle (SDLC).

Respond and mitigate, remediate, or resolve application and website information security incidents using approved procedures and tools, ensuring proper documentation of activities performed and final results in the Department's approved IT service management tools.

Perform and report on vulnerability scans, including monthly evaluation and tracking of threats and vulnerabilities, for DMHC IT applications and websites.

Providing subject matter expertise on secure coding practices, assisting in building related guidelines/standards, and performing manual source code reviews for high risk components.

40% (E)

Risk Management and Incident Response

Conduct information security related confidential investigations as required and serve as the central point of contact to internal and external security investigatory entities.

Conduct regular risk assessments and security audits to identify vulnerabilities and gaps in data protection measures, ensuring continuous improvement.

Maintain comprehensive incident reporting and documentation, analyzing root causes of security incidents, preparing detailed reports, and making recommendations for improvement based on lessons learned.

Collaborate with cross-functional teams, including IT, development, and business units, to evaluate security risks, develop remediation plans, and ensure secure deployment and configuration of cloud resources.

15% (E)

Research and Continuous Learning

Actively pursue continuing education to assure knowledge, skills, and technical competencies are kept up to date, and to stay abreast of emerging technologies and evolving best practices through training courses, self-directed education resources, and independent study. Make use of all available training opportunities to grow and share that knowledge with coworkers.

5% (M)

Other

Represent the ISO on special teams, projects, and other duties as assigned. Perform special assignments, attend meetings, and serve as back-up for peers. Maintain current knowledge in the IT field with emphasis on security services by attending applicable trainings and webinars to understand the current service offerings, as well as emerging technology.

(marginal duties may not exceed 5% of the duty statement)

SUPERVISION EXERCISED OVER OTHERS:

Does not supervise others.

KNOWLEDGE, ABILITIES AND ANALYTICAL/SUPERVISORY REQUIREMENTS:

The employee should be familiar with DMHC mission, goals, organizational structure and major work programs. The employee must also have a demonstrated positive attitude and a commitment to conduct business in a professional manner in dealing with the public and department clients and provide quality customer service to all customers, and be able to deal tactfully, professionally and confidentially with all internal and external customers and contacts.

In addition, the employee must:

All knowledge and abilities of the Information Technology Specialist I classification; and

Knowledge of: Emerging technologies and their applications to business processes; business or systems process analysis, design, testing, and implementation techniques; techniques for

DUTY STATEMENT

DMHC 62-137 New: 12/04 Rev: 05/2023

assessing skills and education needs to support training, planning and development; business continuity and technology recovery principles and processes; principles and practices related to the design and implementation of information technology systems; information technology systems and data auditing; the department's security and risk management policies, requirements, and acceptable level of risk; application and implementation of information systems to meet organizational requirements; project management lifecycle including the State of California project management standards, methodologies, tools, and processes; software quality assurance and quality control principles, methods, tools, and techniques; research and information technology best practice methods and processes to identify current and emerging trends in technology and risk management processes; and state and federal privacy laws, policies, and standards.

Ability to: Recognize and apply technology trends and industry best practices; assess training needs related to the application of technology; interpret audit findings and results; implement information assurance principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data; apply principles and methods for planning or managing the implementation, update, or integration of information systems components; apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality, human resources, communications, and risk and procurement management; monitor and evaluate the effectiveness of the applied change management activities; keep informed on technology trends and industry best practices and recommend appropriate solutions; foster a team environment through leadership and conflict management; effectively negotiate with project stakeholders, suppliers, or sponsors to achieve project objectives; and analyze the effectiveness of the backup and recovery of data, programs, and services.

CONSEQUENCE OF ERROR/RESPONSIBILITY FOR DECISIONS:

The employee may have access to very sensitive and confidential information. Careless, accidental or intentional disclosure of information to unauthorized persons can have far-reaching effects, which may result in civil or criminal action against those involved.

The employee is responsible for complying with the Information Practices Act (IPA) by protecting departmental employees' confidential information, including but not limited to social security numbers, medical or employment history, education, financial transactions or similar information. Failure to protect department employees' confidential information may damage DMHC's reputation as a confidential organization, may result in employee grievances or lawsuits, and, pursuant to California Civil Code section 1798.55, could result in disciplinary action, including termination of employment.

PHYSICAL, MENTAL AND EMOTIONAL REQUIREMENTS:

Employees may be required to sit for long periods of time using a keyboard and video display terminal or traveling in a vehicle to other locations; must be able to organize and prioritize their work under deadline situations and adapt behavior and work methods in response to new information, changing conditions or unexpected obstacles; will be involved with sustained mental

DUTY STATEMENT

DMHC 62-137 New: 12/04 Rev: 05/2023

activity needed for analysis, reasoning and problem solving; must be able to develop and maintain cooperative working relationships, recognize emotionally charged issues, problems or difficult situations and respond appropriately, tactfully and professionally; and must be able to work independently. The employee must be able to create/proactively support a work environment that encourages creative thinking and innovation; understand the importance of good customer services and be willing to develop productive partnerships with managers, supervisors, other employees, and, as required, control agencies and other departments.

WORK ENVIRONMENT:

The DMHC utilizes a hybrid telework model to provide all employees with an avenue to telework while ensuring business and operational needs are met.

Remote-Centered employees are expected to maintain a safe and distraction free work environment at the approved alternate work location. Remote-Centered employees agree to adhere to the state telework policy, the DMHC's telework policy, and conditions cited in the Telework Agreement (STD 200).

Office-Centered employees are expected to maintain a dedicated workstation at a DMHC official worksite. Office-Centered employees are expected to work in a climate-controlled office or cubicle under artificial lighting.

POSITION REQUIREMENTS:

This position requires the incumbent maintain consistent and regular attendance; communicate effectively (orally and in writing if both appropriate) in dealing with the public and/or other employees; develop and maintain knowledge and skill related to specific tasks, methodologies, materials, tools and equipment; complete assignments in a timely and efficient manner; and, adhere to departmental policies and procedures regarding attendance, leave, and conduct.

Note: Any business travel reimbursements will be done in accordance with the approved applicable Memorandum of Understanding (MOU).

ADDITIONAL REQUIREMENTS:

This position is required under the DMHC's Conflict of Interest Code to complete and file a Form 700 within 30 days of appointment and annually thereafter.

SIGNATURES:

The statements contained in this duty statement reflect details as necessary to describe the principal functions of this job. It should not be considered an all-inclusive listing of work requirements. Individuals may perform other duties as assigned, including work in other functional areas to cover absence of relief, to equalize peak work periods or otherwise to balance the workload.

Employee: I have read and understand the duties listed above and can perform them with/without Reasonable Accommodation (RA). *(If you believe you may require Reasonable Accommodation, please discuss this with the hiring supervisor. If you are unsure whether you require Reasonable Accommodation, inform the hiring supervisor, who will discuss your questions and/or concerns with the RA Coordinator.)*

State of California
Health and Human Services Agency
Department of Managed Health Care
DUTY STATEMENT

DMHC 62-137 New: 12/04 Rev: 05/2023

Supervisor: I have discussed the duties with and provided a copy of this duty statement to the employee named above.

EMPLOYEE NAME (PRINT)		SUPERVISOR NAME (PRINT)	
Employee's Signature	Date	Supervisor's Signature	Date