Duty Statement
Department of Managed Health Care

OFFICE: Office of Technology and Innovation	**EFFECTIVE DATE:**
CLASSIFICATION: Information Technology Specialist I	**DATE APPROVED:** **06/17/2024**
POSITION: 521-1402-xxx	**TELEWORK DESIGNATION:** *Remote-Centered*
WORKING TITLE: Security Analyst	

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.

State of California
Health and Human Services Agency
Department of Managed Health Care
DUTY STATEMENT
DMHC 62-137 New: 12/04 Rev: 05/2023

IT DOMAINS

☐ Business Technology Management
☒ Client Services
☐ Software Engineering
☐ IT Project Management
☒ Information Security Engineering
☒ Systems Engineering

TYPICAL DUTIES:

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

PERCENTAGE	JOB DESCRIPTION
Essential (E)/Marginal (M)	
35% (E)	**Procedures and Assessments**

Review, update, and maintain Privacy Program documentation to include Privacy Threshold Assessment/Privacy Impact Assessments and procedures related to the Privacy Policy directives. Communicate with other members of DMHC teams to discuss Business Impact Analysis as well as gather other necessary information to further develop recovery plans.

Maintain and improve DMHC's information security program standards, guidelines, practices, and procedures to align and comply with statewide requirements and goals as outlined in the State Administrative Manual (SAM), the Statewide Information Management Manual (SIMM), IT Technology Letters, and other published and required materials as appropriate.

Develop, document, implement, and follow assigned procedures and components of the DMHC's information security program, including but not limited to Privacy, PIA/PTA, Risk Management, Audit and Compliance Management, Information Security Governance, Incident Management and Reporting, Policy Management, and Security Awareness, Education, and Training.

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

Research, document, and file state-mandated compliance reports to the California Department of Technology according to pre-defined reporting schedules, including but not limited to SIMM 55, SIMM 5305, SIMM 5320, SIMM 5325, and SIMM 5330 reports.

35% (E) **Incident Remediation and Triage**

Use incident response tools and methodologies as well as principles,

policies, procedures and best practices to monitor, maintain, control and protect the Department to ensure the confidentiality, integrity, and availability of production systems and applications.

Respond to security related incidents and provide triage and escalation to facilitate remediation. Work as a cooperative team member with all information technology staff and grow an environment that is easier to manage and troubleshoot for all teams. Build alerts, dashboards, or other tools to provide enhanced system visibility.

Perform ongoing assessments of information security risk and evaluations of information security controls effectiveness. Provide support for incident response, recovery, remediation, and reporting.

Develop and finalize documentation such as management reports, statistical reports, and the status of security and devices within the Department. Monitor laptops, servers, applications, etc for unauthorized or unpatched software. Create reports and work closely with team members to resolve and/or escalate issues.

Stay current with security threats, zero day attacks, and industry trends.

15% (E) **Vulnerability and Risk Management**

Assist in maintaining vulnerability management program. Review Endpoint Defense Reporting incidents to identify risks and anomalies, collaborate and share findings with team members, and recommend solutions to risks identified.

Respond and mitigate, remediate, or resolve 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.

Discover and remediate asset vulnerabilities utilizing endpoint security tools.

10% (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.

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:

Have the ability to reason logically and use analytical techniques to solve difficult problems; research, understand, interpret and articulate applicable laws, rules and regulations; analyze and apply legal principles and precedents to particular sets of facts; provide clear, concise, and effective written documentation and oral presentation.

Knowledge of: Information technology governance principles and guidelines to support decision making; complex and mission critical business processes and systems; principles, methods and procedures for designing, developing, optimizing, and integrating systems in accordance with best practices; system specifications design, documentation, and implementation methodologies and techniques.

Ability to: Formulate and recommend policies and procedures; perform effectively in a fast-paced environment with constantly changing priorities; establish and maintain project priorities; apply federal, state, department, and organizational policies and procedures to state information technology operations; apply systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems; positively influence others to achieve results that are in the best interests of the organization; consider the business implications of the technology to the current and future business environment; communicate change impacts and change activities through various methods; conduct end-user training; collaborate closely with technical subject matter experts such as database administrators, network engineers, and server administrators to ensure systems are secure and meet compliance requirements; assess situation to determine the importance, urgency, and risks to the project and the organization; make decisions which are timely and in the best interests of the organization; provide quality and timely ad hoc project information to executives, project team members, and stakeholders; develop decision making documents; and assess and understand complex business processes and customer requirements to ensure new technologies, architectures, and security products will meet their needs.

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 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.)*

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