Duty Statement
Department of Managed Health Care

OFFICE: Office of Technology and Innovation	**EFFECTIVE DATE:**
CLASSIFICATION: Information Technology Specialist III	**DATE APPROVED:** **07/02/2024**
POSITION: 521-1415-004	**TELEWORK DESIGNATION:** ***Remote-Centered***
WORKING TITLE: **Information Security Architect**	

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. OTI develops, maintains and supports multiple information technology (IT) systems that include a variety of office automation tools, custom applications, public and internal web sites, business intelligence tools, cloud-based services and the underlying information technology infrastructure.

GENERAL DESCRIPTION:

Under the administrative direction of the Information Technology Manager II (Chief Information Security Officer), the IT Specialist III serves as the Information Security Architect for the Department of Managed Health Care. The incumbent is responsible for architecting how current and future solutions will integrate and operate with DMHC systems and applications in the most secure manner. This position is in the Information Security Engineering domain. Duties include, but are not limited to, the following:

IT DOMAINS

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

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

☒ Software 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%	**Application Security Program**

Serves as a master technical Enterprise Solutions Architecture expert advisor to lead the strategic direction for software engineering and application services within the DMHC. Provides master level direction, guidance and mentoring to staff to ensure security standards are met within the software development life cycle (SDLC).

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

Collaborate with 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.

Lead and advise 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.

20% (E) **Application Development (Security)**

Collaborate with Enterprise Application Development team to design, plan, implement a secure continuous integration and continuous deployment (CI/CD) pipeline that enables security enhancements at

every step. Proficient in secure coding best practices. Leads in the analysis and resolution of the most complex problems and performance issues for web applications and services. Assists in triage of other projects/programs and makes technical recommendations to senior-level leadership.

20% (E) **Vulnerability and Risk Management**

Ensure software systems are resilient against cyber threats and vulnerabilities. Utilize expertise in secure coding practices, encryption, access controls, and other security measures to build robust software solutions. Conduct thorough testing and vulnerability assessments to identify and address any potential security weaknesses. Maintain current knowledge of latest security trends and technologies, security software developers contribute to creating secure software that protects sensitive data and mitigates the risk of security breaches.

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.

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

10% (E) **Documentation, Compliance and Reporting**

Document configurations, engineering details, specifications, project documentation, and other artifacts. Upload and manage documentation in document repositories. Report unresolved infrastructure exposures, misuse of resources, and noncompliance to IT Management in a timely manner.

10% (E) **Research and Continuous learning**

Research and evaluate new technology releases for hardware and software and make strategic recommendations for systems and equipment that would allow the DMHC to meet its information technology goals. Maintain a working knowledge of current information security events and trends by attending vendor specific training events, as well as those presented by the Multi-State Information Sharing and Analysis Center or the California Security Operation Center. Evaluate system load and projected usage; plan for and make recommendations to ensure system health. 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.

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

Knowledge of: Development and application of technology in the current and future business environment; emerging technologies and their applications to business processes; policy development; and applications and implementation of information systems to meet organizational requirements.

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. Providing support and information related to IT security products, updates and services provided to the Department. Technical documentation that helps people understand and use a product or service. Documentation can include online help and manuals (system, end-user, and training). Technical writing explains technologies, processes, and products. Evaluations and validations of the effectiveness of an organization’s security controls, including but not limited to those that pertain to all operations, projects, programs, networks, and systems.

Ability to: Research and identify best practice methods and processes to identify current and emerging trends in technology and recommend appropriate courses of action.

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:

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

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