# DUTY STATEMENT

| Employee Name: | |
|---|---|
| Classification:<br>Information Technology Specialist III<br>(Information Security Engineering) | Position Number:<br>580-152-1415-909 |
| Working Title:<br>Information Security Architect | Work Location:<br>1616 Capitol Ave. Sacramento, CA 95814 |
| Collective Bargaining Unit:<br>M01 | Tenure/Time Base:<br>Perm/ Full-Time |
| Center/Office/Division:<br>Information Technology Services Division | Branch/Section/Unit:<br>DCOSB/Security Operations Center |

All employees shall possess the general qualifications, as described in California Code of Regulations Title 2, Section 172, which include, but are not limited to integrity, honesty, dependability, thoroughness, accuracy, good judgment, initiative, resourcefulness, and the ability to work cooperatively with others.

This position requires the incumbent to maintain consistent and regular attendance; communicate effectively (orally and in writing) 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.

## Competencies

The competencies required for this position are found on the classification specification for the classification noted above. Classification specifications are located on the California Department of Human Resource's Job Descriptions webpage.

## Job Summary

This position supports the California Department of Public Health's (CDPH) mission and strategic plan by creating innovative solutions, strengthening partnerships and collaborations, and embracing technology. ITSD leverages data and technology to advance goals and inform action and accountability.

Under general direction of the Information Technology Manager II, the Information Technology Specialist III (ITS III) will work independently as a recognized technical subject matter expert on complex statewide systems at the California Department of Public Health (CDPH). The ITS III will perform duties in the Information Security Engineering and System Engineering Domains.

Member of the Security Operations Center (SOC) team providing expert analysis of cloud and on premises cybersecurity architecture and systems. The ITS III will work with external and internal stakeholders to provide subject matter expertise on technical, functional, and business processes, to design and build a holistic view of an organization's security architecture. The ITS III provides the guidance and approval to build, migrate, and upgrade new and existing CDPH IT security systems and applications. Compliance with State and Federal regulations, policies and commercial best practices related to cloud security.

## Special Requirements

☒ Conflict of Interest (COI)

☐ Background Check and/or Fingerprinting Clearance

☐ Medical Clearance

☐ Travel:

☐ Bilingual: Pass a State written and/or verbal proficiency exam in

☐ License/Certification:

☐ Other:

## Essential Functions (including percentage of time)

**40% (E) Cloud Security Architecture**. Design and support a CDPH Office 365 government Cloud environment, including the maintenance and continuous improvement of a life-cycle security model that develops and maintains the dispositions of information systems, services, and data; and safeguards their confidentiality, integrity, and availability. Identifies and implements new security technologies and best practices available in the CA government cloud and the State O365 offerings including cloud Identity and Access Management (IAM), Email Security suite, Multifactor Authentication (MFA), Business to Consumer (B2C), Business to Business (B2B), Threat Analytics, and more. Interfaces and collaborates with CDPH and Agency IT teams, external IT partners and vendors, and management to design and implement security solutions. Serves as a subject matter expert (SME) on Cloud Security for all CDPH internal and external IT projects and initiatives. Implements the technologies and tools to deliver CDPH's key security management processes by exploring existing enterprise systems and identifying new technologies and tools.

**35% (E) Security Engineering**. Security Operations Center (SOC) security subject matter expert (SME) on projects, and security leadership duties as assigned. Provides expert technical information security guidance on all phases of project management and system development life cycles to ensure efficient and effective delivery of implemented system(s) security components. Will define the scope of work, objectives, tasks, and resources needed to successfully plan IT security projects for the department. Develops documentation, including design diagrams, operating procedures, standard configurations, troubleshooting and cause analysis, reports, inventories, and audit responses.

**20% (E) Incident Response.** Provides expert security instruction and leadership for the incident response teams relating to the security aspects of the initiation, design, development, testing, operation, and defense of IT environments to address sources of disruption, ranging from natural disasters to malicious acts. Analyzes business impact and exposure, based on emerging security threats, vulnerabilities, and risks to recommend IT solutions. Researches, documents, and develops reusable cyber security defense procedures/ playbooks in responding to security incidents. Actively responds to security incidents using playbook and security techniques accordingly.

.

## Marginal Functions (including percentage of time)

**5%** Performs other job-related duties as required. Serve as back-up for peers.

| | | | |
|---|---|---|---|
| I certify this duty statement represents an accurate description of the essential functions of this position. I have discussed the duties and have provided a copy of this duty statement to the employee named above. | | I have read and understand the duties and requirements listed above and am able to perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation may be necessary, or if unsure of a need for reasonable accommodation, inform the hiring supervisor.) | |
| Supervisor's Name: | Date | Employee's Name: | Date |
| Supervisor's Signature | Date | Employee's Signature | Date |
| **HRB Use Only**:<br>Approved By: | Date | | |