DUTY STATEMENT

Employee Name:	Position Number: 580-150-1405-002
Classification: Information Technology Manager I (Information Security Engineering)	Tenure/Time Base: Permanent/Full-time
Working Title: Deputy Chief Information Security Officer	Work Location: 1616 Capitol Avenue Sacramento
Collective Bargaining Unit: M01	Position Eligible for Telework (Yes/No): Yes
Center/Office/Division: Information Technology Services Division	Branch/Section/Unit: Information Security Office

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.

All California Department of Public Health (CDPH) employees perform work that is of the utmost importance, where each employee is important in supporting and promoting an environment of equity, diversity, and inclusivity, essential to the delivery of the department's mission. All employees are valued and should understand that their contributions and the contributions of their team members derive from different cultures, backgrounds, and life experiences, supporting innovations in public health services and programs for California.

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. The Information Technology Services Division (ITSD) leverages data and technology to advance goals and inform action and accountability.

Under the general direction of the Information Technology Manger II (ITM II), Chief, Information Security Office (ISO), the Information Technology Manager I (ITM I) serves as the CDPH Deputy Chief Information Security Officer (DCISO) with direct management responsibility for the Enterprise Data Governance, Data Loss Prevention, and Digital Forensics programs to include the planning, scheduling, and monitoring of staff assignments as well as contractor activities that include providing

the technical and administrative expertise and oversight for the security and privacy aspects of the initiation, design, development, testing, operation, and defense of CDPH electronic and physical data and information technology (IT) environments from sources of disruption, ranging from natural disasters to malicious acts.

The DCISO must continually update their knowledge of the latest information and privacy security tools and concepts.

The ITM I collaborates closely with the CDPH Legal Office, Privacy Office, Departmental and, Program management.

The ITM I will work in the Information Security Engineering Domain.

Special Requirements

- ☒ Conflict of Interest (COI)
- ☐ Background Check and/or Fingerprinting Clearance
- ☐ Medical Clearance
- ☒ Travel: Up to 5% travel to the CDPH Richmond campus and/or other facilities may be required.
- ☐ Bilingual: Pass a State written and/or verbal proficiency exam in
- ☐ License/Certification:
- ☐ Other:

Essential Functions (including percentage of time)

25% **Office Management and Administration:**

Serve as DCISO. Typical duties include planning, scheduling, and monitoring staff assignments; directing technical security staff compliance activities via their managers; advising the Directorate and senior departmental managers of risks that threaten the integrity and effectiveness of CDPH's information systems and data; assisting with, or leading the planning, development, administration, and enforcement of CDPH's information security program components and policies; planning and management of the ISO Office budget and contract expenditures to ensure the necessary tools and staffing are available for the information security program; ISO purchase requests; and ensuring control agency compliance documentation is completed and filed in a timely manner.

Responsible for personnel administration which includes, but is not limited to, hiring and staffing; training and individual development plans; performance evaluations; consultant hiring and management; developing training and mentoring opportunities for fostering team cohesiveness and growth, and ensuring open and transparent communications with staff, internal CDPH programs, and external entities.

20% **Information Security Engineering Activities**

Represent the ISO in engagements with management, analysts and, IT professionals within CDPH, California Department of Technology (CDT), State Office of Information Security (OIS), third-party vendors, and other state or federal entities. Lead or collaborate with ISO team members to initiate and complete various activities for information security and privacy which

include access control; architecture and design; business continuity and technology recovery; data security; forensics; governance; data loss prevention; incident management and response; network and telecommunications; policy development and compliance; risk management; software development; and security awareness and training. Prepare and present reports on the security, integrity, and availability of information systems to various levels of management. Conduct research, requirements gathering, analysis, implementation, and documentation for information security governance and data loss prevention programs. Respond to and coordinate activities for customer inquiries and requests. Maintain effective working relationships with the Office of Legal Services, Privacy Office, Office of Compliance, Human Resources Division, and others to provide a comprehensive umbrella of privacy and security controls, investigative resources, and Public Records Act resources for CDPH.

20% **Data Loss Prevention Management**
Develop, architect, implement, and maintain a comprehensive Enterprise Data Loss Prevention System (DLP) and Management Program. Maintain and optimize ongoing communications and processes with stakeholders to define DLP parameters, rulesets, system monitoring requirements, and event response activities. Develop and provide data loss prevention reporting metrics to CDPH management and oversight agencies, as needed.

20% **Data Governance Management**
Develop, architect, implement, and maintain a comprehensive Enterprise Data Governance Framework and Quality Implementation Roadmap Program. Ensure the framework facilitates the development, implementation, and adoption requirements for data quality standards and improvements, and sensitive data protections via effective policies, standards, principles, metrics, processes, related tools, and data architecture including defining roles, responsibilities, and stewardship accountability of CDPH's principal information assets. Serve as a liaison between programs and ITSD to ensure that data related business requirements for the protection of sensitive data are clearly defined, communicated, well understood, and integrated into operational prioritization and planning. Develop and maintain an accurate inventory of CDPH enterprise information maps, including authoritative systems and owners.

5% **Cybersecurity Audit And Assessment Management**
Lead and manage department and program activities and responses to internal, Oversight Agency, or third-party cybersecurity audits and assessments. Mentor, provide leadership and be a technical resource to Program, Information Security, and IT Operations staff in the execution of and response to security audits and assessments. Conduct and coordinate internal security and risk assessments and monitoring activities of the CDPH enterprise and cloud environments to identify vulnerabilities, threats, and risks within CDPH and outside data custodians' environments, and make recommendations or direct actions to address identified threats, risks, and vulnerabilities.

5% **Electronic Record Forensics**
Facilitate and manage authorized forensic investigations and activities for employee email and internet usage; gather and/or preserve electronic records that may be responsive to Public Records Act requests, litigation, law enforcement requests, or personnel investigations.

Marginal Functions (including percentage of time)

5% Performs other job-related duties as assigned.

☐ 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

HRD Use Only:
Approved By: EH
Date: 10/3/23