

**DUTY STATEMENT**

Employee Name:	Position Number: <b>580-152-1402-909</b>
Classification: Information Technology Specialist I (System Engineering)	Tenure/Time Base: Permanent / Full-Time
Working Title: Identity and Access Management Engineer	Work Location: 1616 Capitol Ave., Sacramento, CA 95814
Collective Bargaining Unit: R01	Position Eligible for Telework (Yes/No): Yes
Center/Office/Division: Information Technology Services Division	Branch/Section/Unit: Technology Integration Services Branch

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 customer focused solutions that are responsive and agile; supporting a modern infrastructure, tools, architecture, and standards; to effectively provide efficient services following service level agreements. The Information Technology Services Division (ITSD) leverages data and technology to create sustainability across CDPH by creating efficient solutions that meet customer expectations and reduce waste. As well as, creating innovative solutions, strengthening partnerships and collaborations, and embracing technology.

Under direction of the Information Technology Manager (ITM) II, Chief, Technology Integration Services Branch (TISB), the Information Technology Specialist (ITS) I provides critical technical oversight for Identity and Access Management (IDM) activities deployed and being deployed at CDPH to ensure the security, integrity, and availability of critical data assets and prepares the Department for the new projects, audits and compliance activities. This includes, but is not limited to, engaging in enterprise governance and risk management activities, creating foundational security architecture frameworks and processes, working with Security Operations Center staff to ensure identity systems monitoring, and making recommendations on improvements and efficiencies.

The ITS I performs duties within the System Engineering and Information Security Engineering domains.

---

**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)**

---

- 35% Responsible for managing Azure cloud services to support organizational operations, to include overseeing the deployment, configuration, and maintenance of Azure resources to ensure they are secure and efficient. Implements Privileged Identity Management (PIM) within Azure to provide just-in-time (JIT) privileged access, enforce FIDO2 authentication, and monitor role activations. Defines and manages roles within Azure, ensuring appropriate permissions and restrictions to enhance security and compliance. Performs regular monitoring and auditing of access logs and security alerts as a critical part of these duties to detect and respond to unauthorized or suspicious activities promptly.

Implements and manages Privileged Access Management (PAM) for data center resources to ensure robust security measures and compliance with organizational policies. This includes administering privileged access controls and protocols, such as just-in-time access and multi-factor authentication, to safeguard critical data center assets. Oversees the approval processes for role activations, ensuring that access is granted only to authorized personnel, and that stringent authentication mechanisms are enforced. Performs regular monitoring and auditing of privileged access activities that are essential to detect and respond to unauthorized access attempts or anomalies swiftly. Maintains detailed logs and conducts periodic reviews to ensure that privileged access to data center resources is tightly regulated and aligned with best practices for data security and operational integrity.

- 25% Performs studies and research analysis related to technology projects; provides information technology consultation in support of business programs; coordinates and consults with users, administrators, and engineers to identify business and technical requirements; develops and sustains cooperative working relationships with project stakeholders; identifies infrastructure

system requirements and recommends technology standards and methods to support organizational needs. Conducts research and performs analysis to recommend system upgrades, cost-effective solutions, and process improvements; troubleshoots, tracks, and conducts root cause analysis of system/database/operational issues. Acts in a leadership role and demonstrates technical versatility for lower-level staff aligning with technological modernization strategies in support of CDPH programs.

- 20% Handles incoming support calls for identity and access; assists users with various inquiries; and delivers timely resolutions to maintain the efficiency of the IT infrastructure both on and offsite. Assists end-users in resolving a wide variety of technical problems, logging and tracking inquiries using a ticketing system while maintaining history records. Documents and maintains workflows for successful issue resolution; identifies, evaluates, and prioritizes end-user problems and complaints to ensure they are successfully resolved.
- 15% Acts as a lead with junior staff when applicable on standard operating procedures for current and new technologies. Mentors junior team members including contractors, providing guidance on best practices, and ensuring adherence to established protocols. Documents and updates standard operating procedures, playing a crucial role in maintaining the consistency and reliability of IT operations. Applies leadership to help foster a collaborative and knowledgeable team environment, enhancing overall service delivery and technical support capabilities within the organization.

#### **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: D.S.

Date: 4/7/25