# DUTY STATEMENT

☐ CURRENT

☒ PROPOSED

| CIVIL SERVICE CLASSIFICATION | WORKING TITLE |
|---|---|
| Information Technology Manager II | Head of IT Operations, ISO, and Enterprise Applications M&O |

| PROGRAM NAME | UNIT NAME |
|---|---|
| Office of Information Services | IT Ops, ISO and Enterprise M&O |

| | POSITION NUMBER |
|---|---|
| 2180 Harvard Street, Suite# 160, Sacramento CA 95815 | **400-175-1406-901** |

| BARGAINING UNIT | WORK WEEK GROUP | BILINGUAL POSITION | CONFLICT OF INTEREST FILER | BACKGROUND CHECK |
|---|---|---|---|---|
| M01 | E | No | Yes | No |

## General Statement

Under the general direction of the Chief Information Officer (CIO), the Information Technology Manager II (ITM II) serves as the senior enterprise technology leader responsible for strategic oversight, governance, and operational performance across three critical functional domains: IT Operations, Information Security Office (ISO), and Enterprise Applications Maintenance and Operations (EAMS M&O). This position provides executive-level leadership to approximately 90 technical and operational staff through three directly supervised IT Manager I positions, each accountable for a distinct operational domain. The ITM II establishes policy direction, drives enterprise risk management and cybersecurity strategy, ensures business continuity, and aligns technology investments with the department's long-range strategic objectives and statewide governance requirements. This position exercises broad decision-making authority with significant organizational impact across departmental IT service delivery, security posture, and enterprise application reliability.

Candidates must be able to perform the following essential functions with or without reasonable accommodation.

| Percentage of Time Spent | Duties<br>Essential Job Functions |
|---|---|
| 30% | **Enterprise IT Operations Leadership and Service Delivery**<br><br>Provides executive-level strategic oversight for all enterprise IT operations and infrastructure services, ensuring the reliability, availability, and performance of critical technology infrastructure including networks, servers, data centers, end-user computing, and service desk operations. Establishes and enforces enterprise service delivery standards, operational policies, and performance metrics (KPIs/SLAs) aligned with department business requirements and statewide IT governance frameworks. Provides strategic direction and approval authority for major infrastructure investments, technology refresh programs, and capital procurement decisions. Oversees enterprise business continuity planning (BCP) and disaster recovery (DR) strategies to safeguard mission-critical systems and services. Partners with executive leadership, program offices, and operational stakeholders to assess enterprise technology requirements and develop IT roadmaps that align capabilities with |

| | |
|---|---|
| | departmental strategic priorities and long-range planning objectives. |
| 20% | **Cybersecurity Strategy, Risk Governance, and Compliance**<br><br>Provides enterprise-wide strategic leadership for the Information Security Office (ISO), establishing cybersecurity policy, governance frameworks, and risk management programs that protect departmental data, systems, and infrastructure. Directs the development, implementation, and continuous improvement of the department's Information Security Program in alignment with California Department of Technology (CDT) standards, National Institute of Standards and Technology (NIST) frameworks, and applicable state and federal regulatory requirements. Exercises enterprise risk ownership authority, including authorization of risk acceptance decisions, security exception requests, and corrective action plans. Oversees compliance with statewide security mandates, audit remediation, vulnerability management programs, and incident response operations. Provides executive sponsorship for security awareness programs, workforce capability development, and cross-agency coordination on threat intelligence and emerging cybersecurity risks. Reports on enterprise security risk posture and program effectiveness to the CIO, executive leadership, and oversight entities as required. |
| 20% | **Enterprise Applications Maintenance, Operations, and Lifecycle Management**<br><br>Provides strategic oversight for the Enterprise Applications Maintenance and Operations (EAMS M&O) domain, ensuring the availability, integrity, and performance of enterprise business applications, legacy systems, and integration platforms supporting department programs and services. Directs application lifecycle management activities including maintenance planning, system upgrades, patch management, and strategic decommissioning decisions. Establishes enterprise application service standards, change management policies, and governance frameworks to reduce operational risk and ensure regulatory compliance. Oversees vendor and contract management activities related to enterprise software agreements, maintenance contracts, and third-party service providers, ensuring accountability and performance against contractual obligations. Provides decision authority for application modernization priorities, technical debt remediation strategies, and cross-platform integration initiatives in alignment with enterprise architecture standards and department strategic direction. |
| 15% | **Budget Planning, Resource Management, and Executive Reporting**<br><br>Provides strategic input for budget development, fiscal planning, and resource allocation across IT Operations, ISO, and EAMS M&O functional domains. Develops and defends annual and multi-year budget proposals, monitors expenditures, and ensures fiscal accountability in compliance with state budgetary guidelines and department financial controls. Oversees workforce planning and organizational |

| | |
|---|---|
| | development across approximately 90+ staff, including succession planning, performance management program direction, and strategic staffing decisions. Serves as the primary advisor to the CIO on enterprise technology risk, service delivery performance, cybersecurity posture, and capital investment priorities. Prepares and presents executive-level briefings, reports, and recommendations to the CIO, department leadership, oversight bodies, and external stakeholders. Ensures compliance with business continuity and operational resilience standards, including maintenance and testing of the department's Disaster Recovery Plan and Continuity of Operations Plan (COOP). |
| 10% | **Personnel Management**<br><br>Plan, organize, direct, and review staff assignments. Provide regular and timely written staff performance appraisals. Counsel staff and initiate disciplinary actions as necessary. Recruit, hire, train, and provide leadership to staff. Ensure full compliance with state and federal laws, rules, regulations, bargaining unit contracts, and policies in all personnel practices, including, but not limited to: hiring, employee development, and management. Identify appropriate long-range plans and goals to address succession planning and knowledge transfer. Establish performance expectations for all staff. Review staff work plans, monitor and evaluate progress, and ensure key milestones are met and on schedule. Develop office goals, strategic and operational plans to meet organizational objectives. Monitor, organize, direct, and evaluate the quality and quantity of the office's work and make changes to ensure a productive work environment. Monitor potential workload bottlenecks and recommend appropriate courses of action. Justify additional staff and approve other resources when necessary. Establish standards for customer service and ensure consistent execution. |
| **Percentage of Time Spent** | **Marginal Job Functions** |
| 5% | Represents the CIO in cross-functional, inter-agency, and statewide technology governance forums. Fosters collaboration between functional IT domains to advance enterprise integration, shared services delivery, and organizational capability. Performs other duties as required by the CIO. |

**Conduct, Attendance, and Performance Expectations**

This position requires the ITM II to maintain acceptable, consistent and regular attendance at such level as is determined at the department's sole discretion; Must be regularly available and willing to work the hours the department determines necessary or desirable to meet its business needs. The ITM II effectively communicates appropriately when dealing with the public and/or other employees of the department; develop and maintain knowledge and skills 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.

## Supervision Received

The ITM II reports directly to and receives general direction from CIO. The incumbent is expected to exercise a high degree of independent judgment and initiative in carrying out the strategic and operational responsibilities of the position. The CIO provides broad policy guidance, approves enterprise-level priorities, and reviews outcomes and overall program performance. Day-to-day direction is self-initiated in alignment with departmental strategic objectives, statewide IT governance requirements, and executive leadership guidance.

## Supervision Exercised

The ITM II directly supervises three (3) subordinate IT Manager I (ITM I) positions, each responsible for a distinct functional domain: IT Operations, ISO, and EAMS M&O. Through this supervisory chain, the ITM II exercises indirect oversight of approximately 90 technical, analytical, and operational staff across all three domains. Supervisory responsibilities include setting performance expectations, conducting performance appraisals, approving leave, and making or recommending personnel actions including hiring, disciplinary, and corrective actions.

## Work Environment, Special Requirements/Other Information, Physical Abilities, Additional Requirements/Expectations, and Personal Contacts

### Work Environment

The incumbent performs work in an open-spaced, partitioned office environment with an assigned office in Sacramento, CA. The office is climate-controlled with natural and artificial light. The incumbent will utilize the computer daily. DIR is currently in a hybrid telework schedule and Incumbent will be required to work on site two days a week.

### Special Requirements/Other Information

DIR does not participate in E-Verify.

### Physical Abilities

The incumbent is regularly required to be in a stationary position for long periods of time and communicate; frequently required to operate a computer for extended periods of time, and to move/transport office items in a safe manner. The incumbent must constantly position self to use standard office equipment.

### Additional Requirements/Expectations

The incumbent must possess or be willing to obtain relevant information security or IT management certifications (e.g., CISM, CISSP, PMP, ITIL) as appropriate to the role. The position may require occasional travel to statewide meetings, oversight forums, or off-site facilities. Must be available for on-call response during critical incidents, system outages, or declared emergencies. Required to complete all mandatory state training including Supervisory Leadership, Ethics, and Information Security Awareness programs. Desirable Qualifications: Knowledge of California statewide IT governance policies and CDT standards; experience managing large-scale IT programs and enterprise infrastructure in a public sector environment; demonstrated experience with NIST Cybersecurity Framework, Federal Information Security Modernization Act (FISMA), or comparable regulatory frameworks; strong executive communication, stakeholder engagement, and policy development skills; experience with IT budget formulation and fiscal accountability in a state agency context; proven track record leading multi-disciplinary technology teams of significant size and complexity.

## Personal Contacts

This position maintains frequent and substantive contact with a broad range of internal and external stakeholders including: the Chief Information Officer (CIO) and department executive leadership; three directly supervised IT Manager I positions and approximately 90 indirect staff; program managers, operational directors, and division chiefs across the department; representatives from the California Department of Technology (CDT), California Cybersecurity Integration Center (Cal-CSIC), and other state oversight bodies; federal agency contacts; external technology vendors, contractors, and managed service providers; legal, procurement, human resources, and fiscal staff; and legislative or audit representatives as required.

## Employee Acknowledgment

*I have read and understand the duties listed above and certify that I possess essential personal qualifications including integrity, initiative, dependability, good judgment, and ability to work cooperatively with others; and a state of health consistent with the ability to perform these assigned duties as described above with or without reasonable accommodation. If you believe a reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for a reasonable accommodation, inform the hiring supervisor who will discuss your concerns with the Medical Management Unit in the Human Resources Office.*

| Employee Name | Employee Signature | Employee Sign Date |
|---|---|---|

## Supervisor Acknowledgment

*I certify this duty statement represents a current and accurate description of the essential functions of this position. I have discussed the duties of this position with the employee and provided the employee with a copy of this duty statement.*

| Supervisor Name | Supervisor Signature | Supervisor Sign Date |
|---|---|---|

## HUMAN RESOURCES OFFICE APPROVAL

| C&S Analyst Initials | Approval Date |
|---|---|