Department of Toxic Substances Control
Position Duty Statement

Classification Title Information Technology Manager II	**Department** Department of Toxic Substances Control (DTSC)
Working Title Deputy Chief Information Officer	**Office/Unit/Section/Geographic Location** Office of Environmental Information Management/ Enterprise Security & Infrastructure Services Branch/ Sacramento Headquarters
Position Number 810-250-1406-001	**Effective Date**

Primary Domain: System Engineering, Secondary Domain: Information Security Engineering

General Statement: Under the administrative direction of the Deputy Director (Chief Information Officer) of the Office of Environmental Information Management (OEIM), the Information Technology Manager II (ITM II) serves as the Deputy Chief Information Officer, backup to the CIO, and Branch Chief over Enterprise Security and Infrastructure Services. The ITM II will cross-functionally manage OEIM Operations in partnership with OEIM Senior Management, DTSC and Agency personnel. The ITM II is responsible for leading and managing the Enterprise Security and Infrastructure Services branch and complex information technology projects. Responsibilities include advising and communicating to the CIO, DTSC executives, division chiefs, program managers, and Agency management on all matters related to the implementation and impact of IT systems and security across lines-of-business activities and the tactical implementation of the IT strategy, processes and methodologies as defined by the CIO. Establish vision, goals, objectives, strategies, and tactical direction for Multi-Cloud and Data Center technologies, Enterprise Security and Infrastructure operations, OEIM Service Level agreements and key performance indicators, and management of OEIM Operational Project Portfolio.
Specific duties include but are not limited to:

A. Specific Activities: Essential (E) / Marginal (M) Functions

40% (E) OEIM Operations, Enterprise Security and Infrastructure Operations Management

Under the direction of the CIO, deliver a clear technology vision, providing strategy and direction to Enterprise Security and Infrastructure Services branch by setting goals, expectations, encouraging leadership, teamwork, collaboration, transparency, and motivating staff at all levels. A supporter and advocate of DTSC's core values, OEIM's team first culture, and customer service-oriented communication and service delivery standards. Promote Department and Agency mission, goals, objectives, policies, processes, and procedures. Direct and oversee OEIM daily operations and production services, including change control, change management, fiscal management, contract management, operations management, resource management and talent management. Plan, organize, and direct the multidisciplinary teams of IT professionals, and manage the workload and resources through subordinate managers and leads. Ensure appropriate staffing levels and skills are assigned to maintain efficient and effective operations to support ESIS service offerings within budgeted resources. Responsible for the resource planning of the work activities related to enterprise security and infrastructure services, including but not limited to: Client Services and Support, Infrastructure Services (Network, Servers, Storage, Wireless capabilities), Telecommunications, IT Asset Management, Multi-Cloud, Data Center and hybrid Technologies, Security Services and Operations, IT Risk Management; Information Security Compliance Management; Incident Management; Privacy and Security Awareness Program; Technology Recovery Planning; and Security Control Audit Program. Implements infrastructure and security strategies and tactical best practices, determined generally by industry best practices, in collaborative partnership with OEIM Management, DTSC and CalEPA (Agency). Evaluates, plans, and determines key performance indicators and develop work plans to increase efficiencies of OEIM's Operations and service levels for enterprise infrastructure and security services. Provides direction on organization's contingency plans for business continuity and continual process improvements. Oversees continuous monitoring of all enterprise security and infrastructure services for technology changes, topology changes, anomalous activity, and other alterations that might impact DTSC business operations. Lead and manage OEIM Operational Project Portfolio in collaboration with OEIM Senior Management and personnel for program prioritization.

15% (E) Service, Risk and Compliance Management & Privacy Program Oversight

Identifies infrastructure and security risks, manages the risk register, and works with System Owners to mitigate identified and future risks throughout the Department. Oversees departmental risk assessments, both internal and external triggered, identifying potential vulnerabilities and its business impact that threaten the security, confidentiality, and integrity of DTSC information assets. Collaborates throughout the Department to identify and estimate the cost of protective measures to mitigate and prevent vulnerabilities to an acceptable level. Participates in the selection of cost-effective security management measures and tools to mitigate security threats. Prepares confidential reports for OEIM Senior Management documenting identified risks, proposed security management measures, resources necessary for security management and residual risk. In collaboration with the Privacy Office, serves as the subject matter expert on privacy policy recommendations, development, reviews and updates. Performs complex business process analysis to ensure enterprise systems and business areas incorporate privacy principles and requirements in accordance with state and Federal mandates. Oversee and support the Privacy Program by identifying privacy weaknesses and propose solutions to appropriate project, IT, or program management. Reviews and updates existing processes for privacy compliance with statewide privacy policies. Identifying privacy compliance issues and supports system owners/custodians in remediation development in compliance with State of California, Agency and DTSC's privacy policies. Handles privacy incidents, completes all facets of the incident response, including, but not limited to, conduct interviews, draft reports, document lessons learned, and address privacy risks or issues in order to resolve incidents in a timely manner and from this data, identifies needed improvements in the design, implementation, and operation of DTSC's privacy program.

15% (E) Infrastructure, Security Program, and Policy Management

Develops, implements, and manages the DTSC's information security program that supports business operations and aligns with the departmental mission, goals, and objectives. Ensures the information security program is compliant with all applicable legal, statutory, and regulatory requirements. Work in collaboration with Chief Information Security Officer (CISO) to identify and improve enterprise infrastructure and security posture, thru security management frameworks such as NIST, FEDRAMP, FIPS, OWASP and SIMM. Serving in partnership with the OEIM Senior Management, establishes security and infrastructure strategy, roadmap(s), and information technology policy for DTSC. Formulates, recommends, and oversees implementation of the Department's enterprise-wide information technology security policies and standards. Oversees and/or directs the implementation of information security policies and practices related to the delivery and protection of information assets. Ensures that the Department is in compliance with State, Agency and DTSC information security policies, standards and requirements. Provides oversight over all information technology security operational activities within the DTSC. Collaborates with departmental executives and senior managers to integrate administrative security controls into Department processes and procedures. Works with various programs to ensure that staff and management comply with the information security policies, standards, and other applicable requirements. Assists, or leads, planning related to emergency preparedness, incident response, and prevention.

10% (E) Personnel Management

Plans, organizes, directs, and provides managerial review of the work performed in the Branch. Provides regular and timely written performance appraisals to staff. Counsels staff and initiates disciplinary actions as necessary. Recruits, hires, trains, develops, and provides leadership to staff. Complies with state and federal laws, rules, regulations, bargaining unit contracts, and policies in all personnel practices. Manages and coordinates assignments of technical staff based on departmental and OEIM priorities, staff experience and skill levels, complexity assessments of projects, specialized skills and experience requirements, and resource availability. Establishes performance standards and expectations by conducting probationary reviews, annual performance reviews, annual Individual Development Plans, constructive intervention, corrective and disciplinary actions, and training to enhance personnel growth. Establishes reasonable deadlines and monitors staff's workload to ensure work is completed accurately and timely. Provides advice and consultation to staff on the most difficult and sensitive work issues. Encourages team building across all service delivery teams. Facilitates cross training and promotes continuous improvement of processes. Implements motivation techniques, promotes training, and creates a positive climate for change. Mentors staff and ensures training opportunities are available to assist in developing technically skilled staff. Sets and communicates standards of performance for all team members. Promote upward mobility and provide equal employment opportunities for a harassment and discrimination-free work environment. A catalytic agent in developing a customer focused service organization.

10% **(E) Research and Training**
Researches and evaluates current and new infrastructure and security technologies and trends. Collaborates with Agency and BDO (Boards, Departments, Offices) IT enterprise architects, and information security teams to assist with the design, implementation and identifying standards for infrastructure and security technical controls or threat countermeasures for projects, systems, and applications. Conducts infrastructure and security assessment to identify gaps and develop alternatives for investment recommendations to improve enterprise-wide security posture in system and technical architecture, and business operations.

5% **(E) Administrative Duties**
Performs administrative duties including, but not limited to: adheres to Department policies, rules, and procedures; submits administrative requests including leave, overtime, travel, and training in a timely and appropriate manner; accurately reports time in the Daily Log system and submits timesheets by the due date.

5% **(M) Team Leadership**
As a member of the OEIM's leadership team, participates in organizational efforts to facilitate the effective management and leadership of the organization. Performs other related duties, as required.

B. Supervision Received
The ITM II reports directly to and receives most assignments from the CIO. The ITM II may also receive technical direction on security policies and activities from the Agency Information Officer (AIO) or Agency Information Security Officer (AISO).

C. Supervision Exercised
The ITM II supervises several subordinate staff in the following classifications: Information Technology Manager I, Information Technology Specialist III, Information Technology Supervisor II, Information Technology Specialist II, Information Technology Specialist I, and Information Technology Associate.

D. Administrative Responsibilities for Supervisors and Managers
The ITM II performs the full range of supervisory and management duties including, but not limited to, interprets and adheres to policies, rules, laws, regulations, and bargaining unit contracts; provides

direction and guidance regarding work assignments and daily work activities to ensure timely completion of assignments; reviews work and evaluates performance of staff by providing regular feedback and completing timely probationary reports, annual performance appraisals, and individual development plans; monitors employee performance and, if necessary, utilizes progressive discipline principles and procedures; completes personnel documentation and utilizes the competitive hiring process; and approves or denies administrative requests including leave, overtime, travel, and training. The ITM II is responsible for developing and monitoring program goals, objective and budget. This level is responsible for the personnel development activities of personnel within the IT unit, contract negations, and business services.

E. Personal Contacts

The incumbent has frequent contact with vendor system experts, systems and network administrators, database system administrators, server application developers, multiple programs within DTSC, project team members, peers, Agency and State Information Officers, and other external consultants, contractors, and vendors. Contacts occur in conferences, meetings, hearings, or presentations involving problems or issues of considerable consequence or importance. Contacts typically have diverse goals or objectives requiring common understanding of the problem and a satisfactory solution by convincing individuals, arriving at a compromise, or developing suitable alternatives. Contacts are to justify, defend, negotiate, or settle matters involving significant or controversial issues.

F. Actions and Consequences

The consequence of error at the ITM II level may have statewide and enterprise-wide impacts. Consequences include lost funding, project failure, failed business strategy, poor customer service and performance, risk exposure, loss of business continuity, missed business opportunity and budget implications.

G. Functional Requirements

The ITM II works in a high rise building with artificial light and temperature control. A flexible work schedule, including telework, is available (the incumbent will be expected to be available through various platforms throughout the day to communicate on work related activities). The ability to use a personal computer and telephone is essential. No specific physical requirements are present. May be required to travel to meetings, training, and the regional offices. The incumbent may work on sensitive, confidential, and controversial assignments. The incumbent must work well with others, accommodate changing priorities, work occasional irregular or extended hours, and be able to meet critical deadlines.

H. Other Information

This position requires the ability to plan, coordinate and direct the activities of technical staff, develop and evaluate alternatives, make decisions and take appropriate action, establish and maintain priorities, effectively develop and use resources, analyze data and effectively communicate ideas and information to staff and management, reason logically and creatively and use a variety of analytical techniques to resolve managerial problems, and successfully gain and maintain the confidence and cooperation of those contacted during the course of work. The incumbent must exhibit punctuality and dependability in executing the duties of this position.

I. DTSC's Equity Statement

The DTSC values diversity, equity, and inclusion throughout the organization. We foster an environment where employees from a variety of backgrounds, cultures, and personal experiences are welcomed and can thrive. We believe the diversity of our employees is essential to inspiring innovative solutions. Together we further our mission to DTSC's mission. Join DTSC to improve the lives of all Californians.

I have read and understand the duties listed above, and I can perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation is necessary, discuss your concerns with your supervisor.)

____________________________________ _____________________
Employee Signature Date

____
Printed Name

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

____________________________________ _____________________
Supervisor Signature Date

____
Printed Name

Approved: