Department of Toxic Substances Control
Position Duty Statement

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

Primary Domain: Information Security Engineering, Secondary Domain: System 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 Chief of the Enterprise Security Services Unit. The ITM II is responsible for leading and managing the security branch of OEIM and complex information technology security projects. Specific duties include, but are not limited to:

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

30% (E) Information Security Office Operations and Management
Responsible for the resource planning of the work activities related to information security, including but not limited to: IT Risk Management; Information Security Compliance Management; Incident Management; Privacy and Security Awareness Program; Technology Recovery Planning; and Security Control Audit Program. Implements information security strategies and tactical best practices determined generally by industry best practices and, more specifically, in collaborative partnership with the Information Security Officer (ISO), OEIM Managers and CalEPA (Agency). Works with project teams and System Owners to ensure all deployments, enhancements, operations, and maintenance of the Department of Toxic Substances Control's (DTSC) network and systems are completely documented, verifiable, and replicable for other information technology professionals. Manages high-level technical security tasks for DTSC and provides timely Security Advisory communications and alerts in support of the ISO and staff**.** Responsible for development of technology and budget change requests based on substantiated needs. Ensures cost-effective use of resources and identify operational cost savings related to information technology security throughout the Department. Evaluates an organization's contingency plans for business continuity strengths and weaknesses. Identifies, captures, contains, and eliminates malware. Oversees continuous monitoring of all enterprise services for technology changes, topology changes, anomalous activity, and other alterations that might impact the security posture of the business entity.

20% (E) Risk and Compliance Management & Privacy Program Oversight
Identifies security risks, manages the risk register, and works with System Owners to mitigate said risk throughout the Department. Oversees departmental risk assessments to identify potential vulnerabilities that could threaten the security, confidentiality, and integrity of DTSC information assets. Collaboratively determines the probable impact of identified threats and assess the likelihood of such occurrences. Collaborates throughout the Department to identify and estimate the cost of protective measures which would eliminate or reduce 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 the ISO or his/her designee documenting identified risks, proposed security management measures, resources necessary for security

management and residual risk. Serves as the subject matter expert on privacy policy development, reviews and makes recommendations to update existing privacy policies. Performs complex business process analysis to ensure enterprise systems and business areas incorporate privacy principles and requirements in accordance with state and Federal mandates. Identifies privacy weaknesses and proposes solutions to appropriate project, IT, or program management. Reviews and updates existing processes for compliance with statewide privacy policies, identifying compliance issues and supports system owners and/or system custodians in the development of step-by-step procedures for remediation and compliance with State of California, Agency and DTSC's privacy policies in order to ensure successful implementation of the Privacy Program. 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) 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.

Serving in partnership with the ISO, establishes information security strategy, roadmap(s), and information security 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.

15% (E) Personnel Management

Plans, organizes, directs, and provides managerial review of the work performed in the unit. 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 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.

10% (E) Research and Training

Researches and evaluates current and new information security technologies and trends. Collaborates with Agency and BDO IT enterprise architects, and information security teams to

assist with the design and implementation of security technical controls or threat countermeasures for projects, systems, and applications. Conducts 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; however, direction and assignments may also come from the Chief Deputy Director or Director. The ITM II may also receive technical direction on security policies and activities from the Agency Information Officer or Agency Information Security Officer.

C. Supervision Exercised

The ITM II supervises several subordinate staff in the following classifications: Information Technology Specialist III, Information Technology Specialist II, Information Technology Specialist I.

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 Date: 9/2021