California Department of Tax and Fee Administration

DUTY STATEMENT

☐ CURRENT
☐ PROPOSED

SCHEDULE TO BE WORKED/WORKING HOURS		EFFECTIVE DATE	

CIVIL SERVICE CLASSIFICATION	PRIMARY DOMAIN	WORKING TITLE
Information Technology Manager I	**Information Security**	**Security Operations Team Manager**

DIVISION/OFFICE/UNIT	SPECIFIC LOCATION ASSIGNED TO
TSD/Security Operations Team	**Headquarters – Sacramento, CA**

SEERA DESIGNATION	BARGAINING UNIT	WORK WEEK GROUP	CERTIFICATES REQUIRED
Managerial	**M01**	**E**	**None**

FINGERPRINTS/ BACKGROUND CHECK REQUIRED	BILINGUAL POSITION	SUPERVISION EXERCISED
☒ Yes ☐ No	☐ Yes ☒ No	**Yes**

INCUMBENT	POSITION NUMBER *(Agency-Unit-Class-Serial)*
	291-381-1405-017

The mission of the California Department of Tax and Fee Administration is to make life better for Californians by fairly and efficiently collecting the revenue that supports our essential public services.

POSITION'S ORGANIZATIONAL SETTING AND MAJOR FUNCTIONS

Under the administrative direction of the Chief Information Officer, the incumbent acts as the technical security expert and manager for intrusion detection, security incident response, and compliance monitoring. The incumbent will have technical responsibility for planning, organizing, coordinating, directing, and controlling the direction of the Security Operations Team (SOT). The incumbent will lead the team in researching and identifying information security trends and technologies.

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

PERCENTAGE OF TIME SPENT	DUTIES
	ESSENTIAL JOB FUNCTIONS
45%	Manages and provides leadership to technical staff on highly technical and sensitive work related to SOT functions; Network Monitoring/Threat Hunting, Vulnerability Management, Administration of SOT tools and Incident Response. Serves as the primary expert and resource in providing support and mentoring while managing the work of technical staff, setting priorities, scheduling work assignments, and making adjustments as necessary due to changing priorities. Works with TSD team members on complex technical issues including troubleshooting of system issues and ensures that TSD leadership are aware of issues that impact business processes. Works with technical staff to respond to identified threats and security violations to departmental systems that may result in unauthorized intrusions, misuse of system resources, or other improper activity. Analyzes activity to determine if events are actual attacks or false positives and implements the appropriate response or corrective action as necessary. Tracks and verifies resolution of identified events and notifies appropriate teams to ensure timely notification to control agencies where required. Plans, prepares, performs, and evaluates vulnerability scans of CDTFA systems and works with technical staff in resolving deficiencies. Manages the recruitment, hiring, training and administrative processes in support of the SOT. Manages staff resources to ensure staffing levels support TSD and the Department's customers and mission.
35%	Serves as the leader in the most complex Information Security projects. Leads team in planning, designing, testing, implementation, and maintenance of projects. Performs research on the most complex intrusion detection and monitoring security issues. Plays a major role in the development of IT security polices and standards including implementation approaches and plans. Leads teams analyzing and determining solutions for implementing security best practices and mitigation of compliance issues and potential security breaches. Presents findings and proposed solutions to TSD leadership.

15%	Provides technical consultation to senior technical staff and TSD Leadership. Identifies and assembles necessary resources to support the Information Security component of complex information technology projects. Evaluates and tests security tools and reports to the ISO and TSD Leadership. Maintains an extensive knowledge and up-to-date perspective on evolving Intrusion Detection System / Intrusion Prevention System / Vulnerability management and Security trends, standards, and best practices. Stays abreast of cybersecurity threats to the Department's information resources and from activities related to unauthorized intrusion attempts and misuse of system resources.
	MARGINAL JOB FUNCTIONS
5%	Works closely with Privacy, Security, and Disclosure teams to build the strategy and vision of CDTFA's Information Security Program. Collaborates on building and defining Security Operations Team's strategic goals.

WORK ENVIRONMENT OR PHYSICAL ABILITIES REQUIRED FOR THE JOB (if applicable):

Work Environment:

- Position is located in a high-rise building

Physical Abilities:

-

Additional Requirements/Expectations:

- Work long or irregular hours as required

I have read this duty statement and fully understand that I must perform the Essential Job Functions of my position with or without reasonable accommodation.

PRINT EMPLOYEE NAME	EMPLOYEE'S SIGNATURE	DATE

I certify that the above accurately represents the duties of the position and that I have reviewed these duties with the above-named employee.

PRINT SUPERVISOR NAME	SUPERVISOR'S SIGNATURE	DATE

HRB Approval Date: August 18th, 2022	**C&P Analyst Initials: GNR**