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	Deputy CISO and Privacy Officer	
DIVISION/OFFICE/UNIT		**SPECIFIC LOCATION ASSIGNED TO**	
Technology Services Division/Information Security Office		Sacramento, CA - Headquarters	
SEERA DESIGNATION	**BARGAINING UNIT**	**WORK WEEK GROUP**	**CERTIFICATES REQUIRED**
Managerial	01	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 general direction of the Chief Information Security Officer (CISO) Information Technology Manager II (IT Manager II), the Information Technology Manager I (IT Manager I) serves as the Deputy CISO & Privacy Officer for the California Department of Tax & Fee Administration (CDTFA). In this role, the Deputy CISO & Privacy Officer provides strategic and operational leadership for information security, cyber risk management, compliance, privacy and business continuity programs, ensuring a well-managed security posture across the department.

The Deputy CISO & Privacy Officer manages the Information Security Office (ISO): Security Governance & Assurance Unit (SGA) and the Security Operations Center (SOC), ensuring governance activities are aligned and integrated with preventative, detective, and corrective security controls. This includes ensuring confidential and sensitive data, such as federal tax information (FTI), personally identifiable information (PII) and other critical assets are properly safeguarded. Close collaboration with IT and business leaders is required to ensure cybersecurity risks are effectively managed and aligned across operational, oversight and assurance functions.

Additionally, the Deputy CISO & Privacy Officer serves as the Privacy Officer, responsible for data protection strategy and execution of policy development, privacy by design, compliance monitoring, incident investigation and breach response. The Privacy Officer ensures adherence to federal and state regulations, reinforcing the department's commitment to data privacy and security.

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

PERCENTAGE OF TIME SPENT	DUTIES
35%	**ESSENTIAL JOB FUNCTIONS** Ensures effective security governance by maintaining adherence to internal information security policies and external regulatory requirements through comprehensive compliance monitoring, enforcement and continuous oversight. Leads the cybersecurity risk management and vulnerability management program forecasting and centralizing risks, enabling informed decision making, accountability and continuous improvement across security governance functions. Coordinates the lifecycle of security audit and assessment findings by ensuring risks are documented, tracked mitigated through structured governance and remediation processes. Develop enterprise-wide security policies, standards, and procedures that align with state and federal requirements including but not limited to the State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), IRS Publication 1075, NIST cybersecurity frameworks and standards, and Information Practices Act privacy requirements. Manages the development, implementation, and management of the Technology Recovery Plan (TRP) as a critical component of the enterprise Business Continuity program to ensure the timely recovery of operations following disruptions caused by technology system outages or declared disasters. Manage the ongoing alignment of the Business Impact Analysis with the Business Continuity program, ensuring that recovery efforts for all business functions are maintained during a disaster, along with emergency response planning initiatives. Assist with audits to ensure compliance with information security policies through the CDTFA's Internal Audit Bureau. Ensures standardization with industry accepted best practices, integrating elements from existing documents, assessing system criticality, and collaborating with relevant stakeholders. Provide leadership and management status and remediation reports during actual disaster events to support IT recovery capabilities. Oversee and coordinate tabletop exercises and recovery drills with both business and technical teams. Coach and mentor the Information Security team to enhance skills, capabilities, and collaboration across the organization. Oversee cybersecurity education and awareness, ensuring staff are equipped to recognize and respond to evolving threats.

35%	Manage security operations, monitoring, detection, analysis and response activities. Ensures response to security alerts and incidents are aligned with operational service level agreements for timely identification, containment and resolution of threats. Assess existing security tools to ensure detection and coverage of adversary techniques are in alignment with frameworks such as the MITRE ATT&CK and cyber intrusion kill chain models. Oversee the design and implementation of custom detection alerts to address coverage gaps, enhancing threat visibility and enabling proactive risk mitigation. Serves as the incident response controller for the CDTFA Cyber Incident Response Team (CIRT) ensuring operational incident response management, planning, and tasking. Ensures CIRT team maintains readiness and technical proficiency aligning with incident response protocols. Coordinates with cross-functional stakeholders and leads alignment of all response streams to analyze, contain and communicate threats. Responsible for delivering situation and investigation reports that capture incident timelines, remediation progress, status of coordination efforts and root cause analysis. Conduct tabletop exercises to test incident response capabilities and readiness. Provide unit level metrics reports for senior leadership. Responsible for staying abreast of technological advancements, industry trends and emerging threats. Collect intelligence sourced information to identify potential risks that may impact the department. Produce actionable intelligence that supports informed decision making and security recommendations. Correlate threat intelligence with security alerts and the vulnerability management program to enable intelligence driven response, patch prioritization, and remediation efforts.
25%	Leads the Privacy Program by providing privacy oversight, policy creation, regulatory compliance, and ensures the protection of confidential and sensitive personal data across the organization. Works with key stakeholders to interpret privacy related issues and questions and coordinates privacy related consultation to customers and program areas when planning or updating any program, system, process, or initiative that involves the collection of personal information. Ensures privacy by design principles are embedded into systems, processes and technologies, safeguarding personal information throughout its lifecycle. Facilitates the data security strategy and execution of secure personal information data handling. Advises and consults leadership and stakeholders regarding privacy requirements and recommendations. Conducts Privacy Impact/Threshold Assessments on systems and applications that collect personally identifiable information. Leads the organization's privacy incident response efforts, coordinating cross functional communication, regulatory notifications, containment and remediation activities and post incident reviews to ensure timely resolution.
	MARGINAL JOB FUNCTIONS
5%	Perform other job-related duties as required.

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

Work Environment:

- Work in a high-rise building.

Physical Abilities:

-

Additional Requirements/Expectations:

-

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: 09/26/2025	**C&P Analyst Initials: LLM**