STATE OF CALIFORNIA
CALIFORNIA DEPARTMENT OF TECHNOLOGY

DUTY STATEMENT

TECH 052 (REV. 02/2018)

RPA NUMBER (HR USE ONLY)
25-112

ALERT: This form is mandatory for all Requests for Personnel Action (RPA).
INSTRUCTIONS: Before completing this form, read the instructions located on last page.

Section A: Position Profile

A. DATE 12/11/2025	B. APPOINTMENT EFFECTIVE DATE	C. INCUMBENT NAME Vacant

D. CIVIL SERVICE CLASSIFICATION Information Technology Manager II	E. POSITION WORKING TITLE Information Security Officer
F. CURRENT POSITION NUMBER 695-330-1406-001	G. PROPOSED POSITION NUMBER (Last three (3) digits assigned by HR) 695-330-1406-001
H. OFFICE / SECTION / UNIT / PHYSICAL LOCATION OF POSITION Internal IT Services/Information Security Office/Rancho Cordova	I. SUPERVISOR NAME AND CLASSIFICATION Quentin Wright, CEA
J. WORK DAYS / WORK HOURS / WORK SHIFT (DAY, SWING, GRAVE) MONDAY-FRIDAY, 8:30 AM -5:00 PM	K. POSITION REQUIRES: FINGERPRINT BACKGROUND CHECK ☒ YES □ NO DRIVING AN AUTOMOBILE □ YES X NO

Section B: Position Functions and Duties

Identify the major functions and associated duties, and the percentage of time spent annually on each (list higher percentages first).

	Information Technology Domains **(Select all domains applicable to the incumbent's duties/tasks.)** □ Business Technology Management □ IT Project Management □ Client Services ☒ Information Security Engineering □ Software Engineering □ System Engineering
	Organizational Setting and Major Functions Under the administrative direction of the Chief Information Officer, the IT Manager II serves as the Department of Technology's (CDT} internal Information Security Officer (ISO). The ISO is responsible for management and oversight of CDT's Information Security Program ensuring protection of CDT's information assets and CDT compliance with state information security policies, standards, and procedures.
% of time performing duties 30%	**Essential Functions** **(Percentages shall be in increments of 5, and should be no less than 5%.)** **Program Management:** Develop, implement, and manage CDT information security program that supports business operations and aligns with CDT's mission, goals, and objectives. Develop, implement, enforce and maintain policies related to the information security program and in relation to its main objectives as listed below. Ensure CDT's information security program is compliant with all applicable legal, statutory and regulatory requirements. CDT's information security program has five main objectives: 1. Protecting CDT's information and information processing assets. 2. Managing vulnerabilities within CDT's information processing infrastructure. 3. Managing threats and incidents impacting CDT's information assets. 4. Assuring through policy the appropriate use of CDT's information assets. 5. Educating employees about their information security and privacy protection responsibilities.
25%	**Risk Management:** Develop, implement, and manage CDT's information security program components including but not limited to security risk management, audit and compliance, information security governance, security incident management program, security awareness education and training.
15%	**Process Management:** Collaborate with CDT executives and senior managers to integrate security administrative controls into departmental processes and procedures.
10%	**Security Architecture:** Collaborate with CDT's information technology, enterprise architecture and information security teams to manage the design and implementation of technical controls and threat countermeasures. Conduct maturity assessments to identify gaps and develop alternatives for investment recommendations to improve CDT's security posture in workforce qualifications system and technical architecture and business processes.
15%	**Strategic Planning:** Ensure CDT's alignment with statewide information security initiatives and lead & participate in security planning sessions.

% of time performing duties 5%

Marginal Functions **(Percentages shall be in increments of 5, and should be no more than 5%.)**

Research and Innovation: Research and evaluate current and new information security technology and trends to develop a departmental information security architecture roadmap

Work Environment Requirements

The incumbent works in an office environment and is required to operate a personal computer, spreadsheet, e-mail communication, presentation, and diagramming applications); use technical software for monitoring a variety of security-related items; and copy machine and telephone system. The incumbent is required to carry a mobile device and may be required to travel when necessary.

Allocation Factors **(Complete each of the following factors.)**

Supervision Received:
The incumbent works under the administrative direction of CDT's Chief Information Officer. Assignments are given in general terms with the desired results and timeliness being specified. The incumbent performs the various phases of the activity including the detail development and scheduling of tasks. The incumbent reviews progress, problems, and changes in priority or schedules with CDT's Chief Information Officer as needed. The incumbent is required to operate with a high degree of independence in performing all duties.

Actions and Consequences:
The incumbent provides in-depth review and analysis of information security standards and best practices to all CDT Offices. The incumbent assists the Department in developing and maintaining confidentiality, integrity and availability to ensure compliance with the State Administrative Manual and federal mandates. Must use discretion while maintaining confidentiality of all personal information.

Personal Contacts:
The incumbent is in personal contact with a wide variety of CDT's executive management, administrative and technical personnel, and vendor community on a daily basis.

Administrative and Supervisory Responsibilities:
The incumbent's administrative duties include preparing status reports on assigned tasks, conducting presentations and meetings, authoring publications as needed, and performing research and analysis.

Supervision Exercised:
The incumbent directly supervises the Security Assurance Information Technology Specialist level staff. Provides general direction concerning assignments.

Other Information

Desirable Qualifications: **(List in order of importance.)**

- Experience in the management of a security program in a highly regulated industry.
- Experience in planning, improving, and implementing large, cross-functional, complex solutions.
- Experience in reporting on sensitive or critical risks and issues to executive management.
- Ability to build strategic relationships with industry-contact in both the public and private sectors.
- Ability to develop and deliver strategic communications and security education programs.
- Experience in conducting enterprise security risk assessments and implementing improvement plans.
- Experience in contract and vendor negotiations.
- Ability to interact with critical staff (such as executive management, the Privacy Officer, the CIO, and the Disaster Recovery Coordinator) and other CDT business units (such as legal, human resources, IT, procurement, business services, and facilities management offices) to cooperatively achieve the goals of CDT.
- Technical competence to lead organization's security Initiatives including knowledge of how technical Issues affect the business of CDT.

INCUMBENT STATEMENT: I have discussed the duties of this position with my supervisor and have received a copy of the duty statement.

INCUMBENT NAME (PRINT)	INCUMBENT SIGNATURE	DATE

SUPERVISOR STATEMENT: I have discussed the duties of this position with the incumbent.		
SUPERVISOR NAME (PRINT)	SUPERVISOR SIGNATURE	DATE