STATE OF CALIFORNIA
CALIFORNIA DEPARTMENT OF TECHNOLOGY

DUTY STATEMENT

TECH 052 (REV. 10/2015)

PROPOSED

RPA NUMBER (HR USE ONLY)
20-281

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	B. APPOINTMENT EFFECTIVE DATE
5/18/21	
C. CURRENT POSITION NUMBER	**D. PROPOSED POSITION NUMBER (LAST THREE (3) DIGITS ASSIGNED BY HR)**
695-312-1401-005	695-330-1405-xxx
E. DIVISION / BRANCH / UNIT / PHYSICAL LOCATION OF POSITION	
Office of Administrative Services / Internal IT Services / Security Assurance / Rancho Cordova	
F. CLASSIFICATION	**G. INCUMBENT NAME**
Information Technology Manager I	Vacant
H. SUPERVISOR NAME AND CLASSIFICATION	**I. POSITION REQUIRES A FINGERPRINT BACKGROUND CHECK**
Keith Parker, Information Technology Manager II (Information Security Officer)	☒ YES ☐ NO
J. WORK DAYS / WORK HOURS / WORK SHIFT (DAY, SWING, GRAVE)	**K. POSITION REQUIRES DRIVING AN AUTOMOBILE**
Monday-Friday / 8AM-5PM / Day Shift	☐ YES ☒ 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).

Organizational Setting and Major Functions

Under general direction of the Information Security Officer, the IT Manager I (IT Mgr I) oversees and ensures functionality of the Department of Technology's (CDT) information security program. The IT Mgr I is responsible for developing, maintaining, and enforcing polices and processes that provide for the integrity, confidentiality and availability of the IT infrastructure and information assets produced or used by the department and its customer agencies.

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

% of time performing duties
40%

Program and Policy Responsibilities

- Develop and implement policies, procedures, and tools to ensure CDT can provide for the safety and security of the technical infrastructure and the data and information of State organizations.
- Develop and implement high-level IT policies and procedures addressing identification, protection, detection, response and recovery mechanisms to protect and maintain the integrity of the technical infrastructure and data files for departmental and program security;
- Ensure overall coordination and integration of CDT security policies, programs and plans.
- Participate directly in setting and implementing complex policies that affect CDT and its customers.
- Advise the Directorate and executive staff on all policy decisions affecting CDT IT security.
- Work in conjunction with executives and management staff from other State departments, industry executives, and control agencies and information security professional organizations in establishing policies that affect the security CDT and its customers.

30%

Manage the most complex administrative and technical project and activities for Security Assurance:

- Implement IT security systems; strategic and operational planning (internal and external).
- Direct Security Assurance's ongoing workload related to Service Desk incident tickets, problem tickets, change requests and security incident response.
- Direct the assurance processes for complex customer projects (server scanning, verification that new applications hosted at CDT meet security standards) prior to application production.

- Develop and present complex material including position papers; budget change proposals and project approval requests.
- Direct the administration and use of security tools for monitoring network and computing resources across CDT.
- Direct the day-to-day activities for the auditing and scanning of network and computing platforms.
- Manage security enforcement efforts and auditing processes (internal and external audits).
- Direct the ongoing vulnerability management processes for CDT including the identification, corrective action, and verification that remediation activities are completed in a timely manner.

30%

Perform day-to-day management activities for Security Assurance:

- Develop plans to accomplish Security Assurance goals and objectives in accordance with organizational mission and strategic goal; support and advocate management's philosophy, policies, and procedures.
- Responsible for making informed and defensible administrative and personnel management decisions in accordance with department and state policies, personnel-related laws, rules, established by CDT administrative processes and procedures, and collective bargaining agreements.
- Encourage unit team building, facilitate cross training and promote continuous improvement of processes. Implement motivation techniques, promote training, and create a positive climate for change.
- Foster methods of creative decision-making and problem solving and provide continuous feedback to management in Security Assurance.
- Advises the Directorate and executive staff and customers on CDT security system solutions for customers' business needs. Forges strong partnerships with customers to understand their business objectives and the impact on the CDT's IT infrastructure.
- Provide leadership and project management on task forces and/or major projects that impact customer departments and/or have department-wide impact.
- Represent Security Assurance at internal and external meetings (customer meetings, the Office of Information Security, the Office of the State Chief Information Officer, and other statewide workgroups.

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

NONE

Work Environment Requirements

- Must pass a fingerprint background criminal record check completed by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).
- Works in a professional environment and is required to operate a personal computer (word processor, spreadsheet, presentation and mail communication).
- Use technical software (as required) for monitoring a variety of security-related items; and photocopy machine and telephone system.

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

Supervision Received:

The IT Mgr I works under the general direction of the Information Technology Manager II.

Actions and Consequences:

Data breaches, security incidents, loss of confidential information, etc.) results in significant risk and liability for the state if appropriate security measures are not developed and enforced.

Personal Contacts:

The IT Mgr I is in personal contact with a wide variety of technical, administrative and department executive staff on a daily basis. External contacts include CDT customers, the CDT, OIS and senior management within customer departments.

Administrative and Supervisory Responsibilities: **(Indicate "None" if this is a non-supervisory position.)**

The IT Mgr I participates in budget activities in regard to security hardware and/or software and will provide input into contracts. The IT Mgr I has responsibility for budget, cost control,

and reporting, and the selection, training, and placement of personnel in Security Assurance under their supervision.

Supervision Exercised:
The IT Mgr I manages Information Technology Specialist classification positions.

Other Information

Desirable Qualifications: (List in order of importance.)

- Well-developed interpersonal skills and the ability to communicate effectively, both verbally and in writing.
- Experience in obtaining buy-in and providing leadership to a large group of multi-disciplinary team members who do not report directly to the IT Mgr I.
- Knowledge of the structure, organization, and function of a variety of technology disciplines, as well as local, State and federal initiatives and programs.
- Ability to anticipate and manage complex issues affecting many organizations, including the ability to develop policy and integrate all aspects of a strategy to assure resolution of issues.
- Proven track record of gaining the confidence and trust of individuals in key positions in the Department's customer base.
- Ability to evaluate products from multiple perspectives (customers, stakeholders, vendors, best practices) in order to develop standards for product approvals.
- Ability to develop/obtain consensus on policy direction that will ensure continuation of the development portion of projects and help ensure successful completion.
- Possession of current CISSP/M and ITIL Foundation and/or Manager Certificates are desired.

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
Vacant		

SUPERVISOR STATEMENT: I have discussed the duties of this position with the incumbent.

SUPERVISOR NAME (PRINT)	SUPERVISOR SIGNATURE	DATE
Keith Parker		