STATE OF CALIFORNIA
CALIFORNIA DEPARTMENT OF TECHNOLOGY
DUTY STATEMENT
TECH 052 (REV. 02/2018)

RPA NUMBER (HR USE ONLY)
26-024 PROPOSED

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	C. INCUMBENT NAME
		Vacant

D. CIVIL SERVICE CLASSIFICATION	E. POSITION WORKING TITLE
Information Technology Specialist II	Information Security Specialist
F. CURRENT POSITION NUMBER	G. PROPOSED POSITION NUMBER (Last three (3) digits assigned by HR)
695-331-1414-015	695-331-1414-015
H. OFFICE / SECTION / UNIT / PHYSICAL LOCATION OF POSITION	I. SUPERVISOR NAME AND CLASSIFICATION
Office of Information Security/Security Operations Center/Solutions Engineering/Rancho Cordova/PG1	Information Technology Manager I
J. WORK DAYS / WORK HOURS / WORK SHIFT (DAY, SWING, GRAVE)	K. POSITION REQUIRES:
Monday-Friday, 8:00am-5:00pm	**FINGERPRINT BACKGROUND CHECK** ☒ YES ☐ NO DRIVING AN AUTOMOBILE ☐ 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).

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 general direction of the Information Technology Manager I (IT Mgr I), the Information Technology Specialist II (IT Spec II) is responsible for leading the ongoing maintenance and support of production security systems and services managed by the Security Solutions Engineering unit. The IT Spec II will have significant responsibilities for technical support for all Office of Information Security (OIS) and other business requests, including Development Security Operations (DevSec Ops) Consulting, Infrastructure/Configuration Management, Automation for "Build and Release" Engineering, database and Data analytics. The IT Spec II will optimize and apply architecture solutions for the benefit of the OIS organization and its statewide partners. The IT Spec II will advise management and formulate information technology security strategy within the organization with a strong focus on DevSecOps principles.

% of time performing duties

Essential Functions

45%

System Development and Operations

The IT Spec II plans and organizes activities of the Security Operations Center (SOC) program areas related to site reliability for all OIS security systems and services.

Site Reliability Engineering

- Work directly with development and operational teams to understand their needs, provide recommendations on infrastructure, and DevSecOps toolchain design, customer and stakeholders needs and then provide technical solutions of the same.
- Drive initiatives to help introduce and improve DevSecOps capabilities that leverage productivity for scalable deployment and automated workflow capabilities, as well as the compilation of data analytics to create dashboards and reports.
- Facilitate continuous integration, continuous deployment, code repository, and webhooks for the development team that include American with Disabilities Act (ADA) and Security review.
- Work with the intake team to establish database automation for onboarding processes.
- Serve as a Subject Matter Expert (SME) on application development teams and groups, representing the division.

Configuration Management/Agile

30%

The IT Spec II leads and oversees complex activities of the architecture team to ensure the architecture is defined, planned, developed, implemented and maintained as defined in requirements, specifications, plans and other documents. Provide problem reports to the appropriate technical support teams as needed.

- Collaborate with Development, Architecture/Engineering, and Operations at all levels to foster successful partnerships critical to the design, development, testing, and implementation of automated/continuous delivery solutions for the Office of Enterprise Technology (OET).
- Work with cross-functional teams to assist in delivering products in a timely manner according to business and technology dependencies.
- Research, implement, and share best practices for configuration management, Infrastructure as Code, and managing cloud/distributed systems.

Intake and Delivery

20%

- Participate in the processes of strategic planning meetings for OET IT efforts.
- Work closely with a variety of staff at all levels within CDT, customer departments, and hardware and software vendors in conducting Proof of Concept (POC) and Value (POV) projects.
- Prepare and present thorough overviews/demos of newly developed applications, prior to implementation to departmental staff.
- Facilitate GitHub CDT source code and account management.
- Lead and participate on Special Projects as assigned by IT Mgr I.
- Advise management and formulate information technology strategy within the organization, with a strong focus on DevOps principles.

Marginal Functions

5%

- Other job-related activities, all staff meetings, share knowledge as requested.

Perform continuous research of cybersecurity technologies & techniques, operating systems, network protection technologies, cloud services, system architecture, systems development lifecycle, and risk management.

Work Environment Requirements

The incumbent works in an office environment and is required to operate a personal computer (word processor, spreadsheet, e-mail communication, presentation, and diagramming applications); use technical software for monitoring a variety of security-related items; and copy machine, fax machine, telephone system. **Must pass a fingerprint background criminal record check completed by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).** This position supports a critical infrastructure team for OIS applications that run 24 hours and 7 days a week. May need to work off hours as events require.

Allocation Factors

Supervision Received:

The incumbent works under the general direction of the IT Mgr I. IT Spec II is expected to complete assignments independently as a technical specialist. The IT Spec II will develop and execute project plans for assignments (including scope of work, identification of internal and external staff stakeholders as well as resources requirements).

The IT Spec II has the responsibility to review progress, report problems, and provide recommendations (i.e. changes in priority or schedules) to OIS and CDT management as necessary. The IT Spec II is required to perform all duties and functions with a very high degree of independence.

Actions and Consequences:

IT Spec II provides the highest level of analysis for the selection of products and services offered to CDT customers. As an external representative of the CDT to its customers, the Government Operations Agency, and the Office of Information Security, the highest degree of professionalism and knowledge of security trends within the CDT customer base and within the industry are required.

IT Spec II possesses knowledge of industry compliance requirements and trends including: FISMA/NIST 800-53, FedRAMP, IRS, CJIS, PCI, HIPAA requirements are essential. The IT Spec II will effectively ensure that Security Solutions' products and services align with customer

security requirements. The inability to perform this function at the mastery level would result in the delivery of inappropriate security services to CDT customers.

Personal Contacts:
The IT Spec II is in personal contact with a wide variety of technical, administrative and CDT executive management on a daily basis. External contacts include CDT customers, the Government Operations Agency, the Office of Information Security, various state and local agencies, and security vendors.

Administrative and Supervisory Responsibilities:
None. However, the IT Spec II may act as lead on a variety of technical duties on the more complex software systems projects.

Supervision Exercised:
This level does not supervise but may lead. The IT Spec II provides technical and project management leadership. The position has defined responsibility and oversight to CDT and statewide stakeholder groups to achieve security goals and develop uniform security policies, procedures and practices.

Other Information

The incumbent must be able to effectively communicate and to fulfill the training needs of staff on new applications and methods. The incumbent must adapt to change within the organization and have general knowledge of the CDT quality culture, core values, vision and mission. The IT Spec II is required to work independently, displaying patience, and professionalism with a variety of individuals of all levels (e.g., Executives, management, peers, and vendors). They must also be reliable and exercise a high degree of initiative, originality, and must demonstrate tact and good independent judgment.

Desirable Qualifications:

- Experience modelling and baselining site reliability configuration items
- Knowledge and experience Implementing High availability for cloud applications and data
- Implementation experience in Database backup and restore in highly scalable infrastructure
- Experience in Database replications across regions and on multi-cloud implementations
- Experience in Databases like MySQL, MS SQL, etc.
- Experience with Microsoft Power Platform (Power Apps, Power BI, Dataverse, etc.), Dynamics, Planner.
- Experience in multi-cloud environments (Azure, AWS, GCP)
- Network administration experience in multi-cloud environments (Azure, AWS, GCP)
- Lead experience in maintaining system logs, hardware/software licenses, and agreements
- Experience working with agile development teams in continuous integration / continuous release cycles model such as AzureDevOps, Phantom, Ansible, Jenkins to maximize efficiency.
- Experience in infrastructure automation/Configuration Management, including but not limited to: Ansible, CloudFormation, PowerShell, Terraform, and Azure Resource Manager.
- Knowledge/Experience with Logging and Monitoring (e.g. Azure monitor, Splunk, Kibana, Monitis, Cloudwatch, New Relic, Datadog, etc.)
- Excellent communication and customer service skills are essential.
- Knowledge of agile project management tools such as (Jira, Pivotal Tracker, AzureDevOps)
- Ability to use a wide variety of open-source technologies and tools.
- Strong grasp of automation tools.
- Knowledge of both Windows and Linux Administration.
- Analytical skills to use data for the benefit of their product and service.
- Experience in time management to meet product/project timelines.
- Demonstrated strong problem-solving skills to reach a solution in an organized manner.
- Ability to effectively communicate and influence people and teams for increased collaboration.

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