**PROPOSED**

|  |  |
| --- | --- |
| State of CaliforniaCalifornia department of technologyDuty StatementTech 052 (Rev. 02/2018) | **RPA NUMBER (HR Use Only)** |
| 21-042 |
| **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 |
| October 13, 2021 |  | VACANT |
| d. CIVIL SERVICE CLASSIFICATION | e. POSITION WORKING TITLE |
| Information Technology Specialist II | Information Technology Specialist II |
| F. Current Position Number | G. proposed Position Number (Last three (3) digits assigned by HR) |
| 695-331-1414-004 |  |
| H. office / section / unit / physical Location of Position | I. supervisor Name and classification |
| Office of Information Security/ Security Solutions Administration/Rancho Cordova | Douglas Novak, Information Technology Manager I |
| J. Work Days / Work Hours / work shift (day, swing, grave) | K. Position Requires:  | fingerprint background check | [x]  Yes [ ]  No |
| Monday-Friday, 7:00am-4:00pm  | 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[x]  Information Security Engineering | [ ]  IT Project Management[ ]  Software Engineering | [ ]  Client Services [x]  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 the ongoing maintenance and support of production security. The Security Solutions Administrative (SSA) team supports and maintains internal and statewide cybersecurity solutions within the California Department of Technology (CDT) data centers and commercial/government cloud environments. Additionally, the SSA group will offer various scalable ubiquitous and subscription services such as vulnerability management, security awareness, phishing programs, and endpoint protections to the Executive Branch of California state government organizations, all fifty-eight counties, city and local governments. |
|  | **Essential Functions (Percentages shall be in increments of 5, and should be no less than 5%.)** |
| **50%** | System Administration and Operations* Serves as a technical lead to the Security Solutions Administration team.
* Provides team member training and mentorship.
* Leads all SSA project and operational tasks.
* Provides and leads SSA technical staff in Cross-functional collaboration with OIS management, oversight agencies, and partners as required.
* Support and maintain internal and statewide cybersecurity solutions within the California Department of Technology (CDT) data centers and commercial/government cloud environments including Amazon Web Services (AWS), Microsoft Azure, and others.
* Work with CDT resources, Customers, and Vendors to maintain security and related systems and services.
* Install, update, and troubleshoot systems/servers.
* Monitor and maintain system/server configurations.
* Manage accounts, authentications rights, and access to systems and assets.
* Provide ongoing optimization and problem-solving support to Customers.
* Develop and document systems administration standard operating procedures.
* Comply with CDT organization systems administration and standard operating procedures.
 |
| **45%** | **General Duties*** Support configure and optimize software, system/server performance.
* Demonstrate technical diagnosing connectivity problems.
* Architect and configure software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware.)
* Support conducting system/server planning, management, and maintenance.
* Provide corrective technical solutions that affect system/server performance.
* Participate in troubleshooting failed system/server components.
* Participate in identifying system/server performance, availability, capacity, or configuration problems.
* Participate in recovering failed systems/server. (e.g., recovery software, failover cluster replication, etc.).
 |
|  | **Marginal Functions (Percentages shall be in increments of 5 and should be no more than 5%.)** |
| **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.
* Develop and present required material including issue memos; position papers; technical analysis; status.
 |
|  | **Work Environment Requirements**The incumbent works in an office environment and is required to:* Successfully complete (pass) a fingerprint background criminal record check completed by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).
* 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.
* .
* 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.
* Required to carry and use a cell phone or mobile device and respond in a timely manner.

**Allocation Factors (Complete each of the following factors.)** **Supervision Received:**The IT Spec II works under the general direction of the IT Mgr I. The 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:**The 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.The IT Spec II possesses knowledge of industry compliance requirements and trends. The IT Spec II will effectively ensure that Security Solutions’ products and services align with customer security requirements. **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: (Indicate “None” if this is a non-supervisory position.)**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:**None, however, the IT Spec II will provide leadership and oversight to CDT and statewide stakeholder groups to achieve security goals and develop uniform security policies, procedures and practices.**Other Information**This position requires:The Information Technology Specialist II works closely with a variety of staff at all levels within the California Department of Technology (CDT), customer departments, and hardware and software vendors. The incumbent must be able to effectively communicate and to fulfill the training needs of staff on new applications and methods. Incumbent must also prepare and present thorough overviews/demos of newly developed applications, prior to implementation, to departmental staff. The incumbent must adapt to change within the organization and have general knowledge of the CDT quality culture, core values, vision and mission. The Information Technology Specialist 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). The Information Technology Specialist II must be reliable and exercise a high degree of initiative, originality, and must demonstrate tact and good independent judgment.**Desirable Qualifications:*** Knowledge of computer networking concepts and protocols, and network security methodologies.
* Demonstrated 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 in multi-cloud environments (Azure, AWS, GCP)
* Lead experience in maintaining system logs, hardware/software licenses, and agreements
* Knowledge of risk management processes (e.g., methods of assessing and mitigating risk).
* Knowledge of laws, regulations, polices, and ethics as they relate to cybersecurity and privacy.
* Knowledge/Experience with logging and monitoring.
* Knowledge of measures or indicators of system performance and availability.
* Knowledge of performance tuning tools and techniques.
* Knowledge of server and client operating systems.
* Knowledge of systems administration concepts.
* Knowledge of enterprise information technology (IT) architecture.
* Knowledge of the type of and frequency of routine hardware and software maintenance.
* Knowledge of Virtual Private Network (VPN) security.
* Knowledge of virtualization technologies including virtual machine and Storage area network (SAN) development and maintenance.
* Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rule, access control).
* Knowledge of system administration, network, and operating system hardening techniques.
* Knowledge of operating systems command-line tools (DOS, UNIX/Linux, Powershell).
* Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS).
* Knowledge of organizational units in Active Directory (AD) and managed user security with group policies.
* Ability to use a wide variety of open-source technologies and tools.
* Strong grasp of automation tools.
* Have strong analytical skills to use data for the benefit of their product and service.
* Strong time management skills to meet product/project timelines.
* Demonstrated strong problem-solving skills to reach a solution in an organized manner.
* The 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 |
| Douglas Novak |  |   |