DUTY STATEMENT
DSH3002 (Rev. 11/2022)

California Department of State Hospitals

Box reserved for Personnel Section

RPA #	C&P Analyst Approval	Date

Employee Name	**Division** Technology Services Division			
Position No / Agency-Unit-Class-Serial 461-104-1414-002	**Unit** Information Security Office			
Class Title Information Technology Specialist II Working Title: Security Specialist	**Location**			
Subject to Conflict of Interest ☒Yes ☐No	**CBID** **R01**	**Work Week Group: E**	**Pay Differential**	**Other**

Briefly (1 or 2 sentences) describe the position's organizational setting and major functions

Under the general direction of the Information Technology Manager I, Information Security Office, the Information Technology Specialist II performs a wide variety of tasks in support of Department of State Hospitals, requiring innovative problem-solving within broadly stated and non-specific guidelines that are essential to the mission of the Department of State Hospitals.

The primary duties of the IT Specialist II lie within the **Information Security Engineering** and **System Engineering** domains. Elements include: security aspects of the initiation, design, development, testing, operation, and defense of information technology data and environments to address sources of disruption, ranging from natural disasters to malicious acts; and, the architecture, design, configuration, operation and maintenance of systems discovery and planning, design, configure, administer, and sustaining the operation of a defined system. System elements include network, server, storage, operating system, database, program, hardware and software.

This position may require 5% travel to any six (6) Department of State Hospital locations.

% of time performing duties	**Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first; percentage must total 100%. (Use additional sheet if necessary).**
30%	**Security Infrastructure Management and Design:** • Acts as the technical lead of the Security Operations team. This includes configuration, architecture, monitoring and responding to alerts from network, server, email, and endpoint protection tools. • Performs analysis of best practice and emerging concepts in security automation • Incident Response • Acts as a technical liaison between clients, service engineering teams, and support staff. • Defines common business and development processes, platform and tool usage for both enterprise/mobile solutions and delivery. • Reviews and audits existing solution design and systems architecture. • Plans, designs, procures, tests, installs, configures, monitors, and maintains the Department's complex network/server security environment.

	• Works with the Information Security Officer and business representatives to research network security technologies. • Develops networking and server architecture that is secure and reliable. • Develops scripts/building tools to support engineering teams, product owners, and other fellow members of the group. • Collaborates with engineering groups, product & project managers, Quality Assurance, and fellow operational teams to architect and develop strategic and tactical solutions. • Continuously improves State Hospital infrastructure for ease of use and scalability while implementing secure and fault-tolerant solutions. • Leads efforts to evaluate new tools and technologies, while utilizing leading edge techniques and knowledge into use for our own operational stack.
30%	**Systems Maintenance and Operations:** • Performs Domain level server administration of the Department's Physical/Virtual Servers in support of security tool deployment • Performs scripting (such as PowerShell) to perform more complex searches or other data manipulation • Performs security inspection of the Department's Windows Server and Network Infrastructure, utilizing Windows tools, vulnerability assessment tools, or other tools as appropriate. • Performs security reviews of Infoblox IP Address Management (IPAM) and DNS Server resources. • Maintains proficiency in the following technologies: Endpoint Protection, Vulnerability Scanning, Email Protection, Network Access Control, Splunk Enterprise Security, Web Protection, Firewall, File Management Tools, Web Access Firewalls, Datacenter Firewalling. • Plans, designs, procures, tests, installs, configures, monitors, and maintains the Department's complex network security environment. • Works with the Information Security Officer and business representatives to research network security technologies. • Development of Network and Server infrastructure security policies. • Ensures that end-user education meets the business requirements of the Department and are consistent with industry best practices and California State security policy.
25%	**Architecture and Staff Mentorship:** • Acts as a consultant or technical advisor in meetings. • Conducts training of new staff to various units in the Department. • Creates/implements and/or modifies service level agreements. • Prepares/reviews project status reports and project implementation plans. • Develops contingency plans. • Leads and mentors the technical team. • Cloud Management of security settings within Azure, Amazon Web Services, and Google Cloud.
10%	**IT Project Management:** • Assesses the requirements of Information Security Unit projects and

	recommends suitable IT components. • Analyzes different options and recommending the most suitable for the project economically feasible. • Works on improving the IT infrastructure of the department. • Recommends upgrades and new systems that will incrementally improve Departmental security posture. • Prepares cost estimates of IT infrastructure. • Consistently monitors the budget and ensures that budget limits are not exceeded. • Formulates procedures and policies for optimum utilization of IT infrastructure resources. • Supervises IT staff, consultants, vendors and suppliers. • Meets with managers of different DSH divisions to assess IT security needs. • Meets with IT analysts and finalizes essential IT infrastructure needs. • Plans and supervises installation of IT infrastructure. • Ensures that the infrastructure development project is completed within the given time frame.
5%	Assists with other Information Technology Specialist II job-related work as requested by management.
Working Conditions	This position is eligible for a hybrid schedule, which includes up to 3 days of remote work per week but is subject to change based on Department guidelines and business needs. The incumbent may travel throughout California as needed, with prior notice. Independence of action and the ability to manage time and multiple priorities is required. Use of technology, including but not limited to Microsoft Office, Microsoft Teams, WebEx, Zoom, and other virtual platforms is required. Incumbent may be required to sit for long periods of time using a keyboard and video display terminal or when traveling to other locations; travel may be required to DSH facilities. **If incumbent works at a hospital, this position requires clearances of Live Scan and Medical Evaluation prior to being hired.**
Other Information	Regular and consistent attendance is critical to the successful performance of this position due to the heavy workload and time-sensitive nature of the work. The incumbent routinely works with and is exposed to sensitive and confidential issues and/or materials and is expected to maintain confidentiality at all times. The Department of State Hospitals provides support services to facilities operated within the Department. A required function of this position is to consistently provide exceptional customer service to internal and external customers. Incumbent must be able to develop and maintain cooperative

working relationships, recognize emotionally charged issues, problems or difficult situations and respond appropriately, tactfully and professionally; and must be able to work independently. The incumbent must be able to create/proactively support a work environment that encourages creative thinking and innovation; understand the importance of good customer services and be willing to develop productive partnerships with managers, supervisors, other employees, and control agencies and other departments.

The Technology Services Division (TSD) plays a significant role in ensuring continuity and quality of DSH's and its hospitals and psychiatric programs delivery of services and patient care through the delivery of highly effective IT service delivery systems. Consequence of error may result in minor to major IT service unavailability or ineffectiveness, causing direct impacts to the delivery of care to DSH patients. A required function of this position is to consistently provide exceptional customer service to internal and external customers.

Statement of Economic Interests / Form 700 Requirements:
The Political Reform Act requires employees who serve in this position to file a Statement of Economic Interest (Form 700) as designated in the department's conflict-of-interest code. Your Form 700 is due within 30 days of assuming office/position, annually, and within 30 days of leaving office/position. The annual Form 700 due date is determined by the Fair Political Practices Commission and is generally due on or about April 1 of each year. The statements must be submitted to the Sacramento Filing Officer. These statements are public access documents. You will receive reminders from the Sacramento Filing Officer regarding completion of the statements; however, it is your responsibility to ensure you are compliant with all regulations and requirements. For additional information regarding the Statement of Economic Interests or regulations, please contact the Sacramento Filing Officer.

Ethics Training and Compliance:
Pursuant to Assembly Bill 3022 and Government Code 11146.4, employees required to file a Form 700 Statement of Economic Interests must complete an Ethics orientation training course within six months of assuming a Form 700 designated position, and every two (2) years thereafter, by December 31 of each even numbered year. The Ethics training governs the official conduct of state officials. You will receive reminders from the Sacramento Filing Officer regarding completion and documentation of the training; however, it is your responsibility to ensure you are compliant with the required training. Your Ethics training record and certificates of completion are public access documents. For additional information regarding the Ethics training and regulations regarding this requirement, please contact the Sacramento Filing Officer.

I have read and understand the duties listed above and I certify that I can perform these duties and the essential functions of this position with or without reasonable accommodation. (If you believe reasonable accommodation is necessary, discuss your concerns with the Office of Human Rights).

	_____ _____ Employee's Signature Date I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above. _____ _____ Supervisor's Signature Date