DUTY STATEMENT
DSH3002 (Rev. 11/2022)

California Department of State Hospitals

Box reserved for Personnel Section

RPA #	C&P Analyst Approval	Date

Employee Name vacant	**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: Senior Security Specialist	**Location** DSH-Sacramento			
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 in the Information Security Office, the Information Technology Specialist II - **Senior Security Specialist** performs a wide variety of tasks in support of the California Department of State Hospitals (CA-DSH), requiring regular innovative problem-solving within broadly stated and non-specific guidelines The primary duties of the IT Specialist II lie within the **Information Security Engineering** and **System Engineering** domains. Elements. Primary responsibilities include supporting the security aspects of the design, development, operation, and defense of IT systems and data, ensuring confidentiality, integrity, and availability while addressing disruptions ranging from natural disasters to malicious acts. Incumbents should also understand the duties required to ensure that all system components comply with federal healthcare regulations, including the Health Insurance Portability and Accountability Act (HIPAA), as well as state requirements such as the Statewide Information Management Manual (SIMM) and the State Administrative Manual (SAM) Section 5300. System components include networks, servers, storage, operating systems, databases, applications, and all applicable hardware and proprietary software.

% 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 sheets if necessary).**
35%	**Technical Leadership, Systems Governance, Security Infrastructure Management and Design** • Technical leadership includes, but is not limited to Incident Response, performing analysis of best practice and emerging concepts in security and automation, and act as a technical liaison between clients, service engineering teams and support staff. • Leads risk assessments, vulnerability management, and security audits. Proactively identify and mitigates potential threats while ensuring compliance with federal and state cybersecurity regulations such as, but not limited to: NIST, HIPAA, CJIS, SIMM, and SAM5300. • Responsible for establishing and enforcing IT security and infrastructure governance frameworks to ensure compliance with state technology policies and regulatory guidelines. This includes overseeing audits,

	assessments, and reporting to executive leadership and regulatory bodies to maintain transparency and accountability in security and infrastructure operations. • Reviews and audits existing solution designs and systems architecture, and develops secure, reliable network and server architectures that align with organizational and security requirements. Continuously enhances the CA-DSH infrastructure to improve usability and scalability while implementing secure, resilient, and fault-tolerant solutions. • Provides leadership in collaborating with engineering teams, product and project managers, quality assurance, and operational groups to architect and drive the development of strategic and tactical solutions. • Provides leadership in research efforts, evaluate, and recommend new tools and technologies, integrating leading-edge techniques and industry best practices into CA-DSH's operational environment to enhance overall capability and performance. • Acts as a consultant and technical advisor, providing expert guidance on security and system architecture decisions, influencing best practices, and supporting teams in resolving complex technical challenges. • Performs security reviews of technical infrastructure by assessing configurations, access controls, and operational practices to ensure secure and reliable network services and conducts security inspections of the Department’s Windows Server and network environments using appropriate toolsets.
30%	**Threat Management, Systems Maintenance and Operations** • Acts as a consultant and technical advisor, leveraging a strong understanding of scripting technologies to guide automation efforts, streamline workflows, and support teams in resolving complex security and systems challenges. • Reviews system and application architectures to identify security gaps and formally recommends improvements to strengthen overall enterprise resilience. • Aids in the design, procurement, testing, installation, configuration, monitoring, and maintenance of the department’s complex security infrastructure. • Maintains proficiency in key security technologies, including but not limited to endpoint detection and response (EDR), Zero Trust frameworks, patch management, certificate management and PKI, Data Loss Prevention (DLP), IP Address Management and Domain Name Service security roles, Security Information and Event Management (SIEM), vulnerability scanning, email security, network access control, web protection, file management tools, web application firewalls, remote access security, network segmentation, Cloud Security, and data center firewalling. • Develops and maintains runbooks, standard operating procedures, and documentation for system operations and maintenance activities. Implements system patches, hotfixes, signature updates, and configuration adjustments in accordance with CA-DSH

	change-management processes, state security policies, and federal healthcare compliance requirements (HIPAA, CJIS, NIST).
15%	**Staff Development, Collaboration, and Technical Leadership** • Leads technical discussions, workgroups, and collaborative planning sessions with other CA-DSH divisions to ensure consistent application of security standards and alignment with departmental goals. • Acts as a consultant and technical advisor, applying strong scripting expertise to drive automation, streamline workflows, and support teams in resolving complex security and systems challenges. • Contributes to the development, revision, and enforcement of CA-DSH cybersecurity policies, standards, and procedures in alignment with state and federal governance requirements. • Ensures that end-user education meets the Department's business requirements and aligns with industry best practices and California State security policies. • Assists in ensuring enterprise systems meet audit, compliance, and oversight requirements such as HIPAA, CJIS, FIPS, and Department of Technology security mandates. • Develops training materials, workshops, and knowledge-transfer sessions to improve team proficiency with security tools and emerging technologies. • Assists management in evaluating staff skill gaps and recommending training priorities, tools, and development opportunities.
15%	**Project Management and Implementation** • Coordinates with internal IT teams, hospital leadership, clinical operations, and external vendors to ensure project alignment and minimize operational disruption. • Collaborates with division managers, clinical and administrative stakeholders, and technical teams to assess security needs and ensure project alignment with hospital operations. • Monitors project progress, tracks deliverables, and ensures milestones are met; identifies obstacles and recommends corrective actions to keep initiatives on schedule. • Ensures project milestones, deliverables, and timelines are met, escalating risks or delays and recommending corrective actions when needed. • Ensures that security systems and infrastructure implementations comply with SIMM requirements, California Department of Technology policies, HIPAA regulations, and internal CA-DSH standards • Prepares cost estimates, budget justifications, procurement specifications, and supporting documentation for security-related acquisitions. • Oversees vendor activities, installation work, technical deliverables, and post-deployment validation to ensure quality and contract compliance.

	• Develops project plans, implementation strategies, timelines, and risk assessments for security upgrades, system integrations, and modernization efforts. • Conducts post-implementation reviews to verify project objectives were achieved and to identify lessons learned and opportunities for improvement.
5%	• Assists with other Information Technology Specialist II job-related work as requested by management.
Working Conditions	This position reports to the Allenby Building in Sacramento. A hybrid Telework schedule, consistent with the State of California's in-office requirement, may be considered with prior approval from management. The incumbent may also be required to travel up to 10% 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. Incumbents 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 CA-DSH facilities.
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. Incumbents 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 can perform these duties 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