DUTY STATEMENT

CDCR INSTITUTION OR DEPARTMENT	POSITION NUMBER (Agency – Unit – Class – Serial)
California Correctional Health Care Services	042-036-1414-973
UNIT NAME AND CITY LOCATED Information Technology Services Division Infrastructure Services, Security Operations, Elk Grove, CA	CLASSIFICATION TITLE Information Technology Specialist II WORKING TITLE Cyber Defense Infrastructure Support Specialist

COI	WORK WEEK GROUP	CBID	TENURE	TIME BASE
Yes ☐ No ☒	E	R01	LT	FT

SCHEDULE (Telework may be available): _____ AM to _____ PM. (Approximate only for FLSA exempt classifications)	SPECIFIC LOCATION ASSIGNED TO 8260 Longleaf Drive, Elk Grove, CA 95758
INCUMBENT (If known)	EFFECTIVE DATE

California Department of Corrections and Rehabilitation (CDCR) and California Correctional Health Care Services (CCHCS) are committed to transforming the correctional landscape to create safer, more professional, and more fulfilling environments for our employees, the incarcerated population, and those supervised in our communities. Through systemwide improvements grounded in proven and emerging practices, we aim to strengthen rehabilitation, enhance workplace satisfaction, and support successful reentry into the community through our institutions, parole, and community partnerships. Our shared mission is to promote safety, wellness, and human dignity while fostering positive change for all those who live and work within our institutions and communities.

CDCR and CCHCS are committed to building an inclusive respectful workplace. We are determined to attract and hire candidates from all communities and empower employees from a variety of backgrounds, perspectives, and personal experiences. We are proud to foster inclusion and drive collaborative efforts at all levels of the Department.

Across our organization, our programs work cooperatively to provide the highest level of health care possible to a diverse correctional population. We encourage creativity and ingenuity while treating others fairly, honestly, and with respect, all of which are critical to the success of the CDCR and CCHCS mission.

PRIMARY DOMAIN:	Information Security Engineering

Under the general direction of the Information Technology (IT) Manager I, the IT Specialist II serves as the Lead Cyber Defense Infrastructure Support Specialist (CDISS), demonstrating a depth of leadership and expertise while performing various complex tasks in support of the overall security posture.

The Lead CDISS will optimize and apply architecture solutions for the benefit of the overall organization and heavily participates in advising and/or formulating information technology strategy and policy within the Department. The existing infrastructure includes various software solutions including but not limited to: Cisco Firepower Threat Defenses, Cisco Security Cloud Control, Cisco Umbrella, Azure Security, Netskope, Illumio, NSX (network virtualization platform), Terraform, Palo Alto.

The incumbent must maintain confidentiality of information acquired while performing job duties, demonstrate ethical behavior, and work cooperatively. Travel to institutions and after-hours support of California Correctional Health Care Services (CCHCS) software applications and systems may be required due to operational needs.

% 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. *(Use addition sheet if necessary)*

	ESSENTIAL FUNCTIONS
40%	Oversees the design, implementation, and maintenance of enterprise network security controls across all current and future platforms. Configures and maintains security rule sets, network zones, segmentation policies, and traffic flow protections to ensure secure communication between environments and prevent unauthorized access utilizing both vendor portals and Infrastructure as Code processes. Utilizes intrusion detection and prevention capabilities to monitor network activity, analyze alerts, and implement appropriate threat-blocking actions. Establishes and maintains secure encrypted communication channels—including remote access solutions and inter-site secure tunnels—to ensure confidentiality of data across untrusted networks. Performs vulnerability assessments, security audits, and timely updates of network security technologies to reduce exposure to emerging risks. Participates in architecture review boards and formal change control processes, ensuring network security modifications align with organizational requirements, compliance standards, and long-term strategic direction
30%	Serves as a technical authority for policy implementation across all network security platforms. Reviews organizational requirements and translates them into enforceable, platform-agnostic security policies, including creating new rulesets, adjusting existing controls, and ensuring alignment with industry best practices. Conducts routine analysis of system logs, dashboards, alerts, and performance indicators across security tools to identify emerging vulnerabilities, operational issues, or unauthorized access attempts. Configures security clients, agents, or enforcement points for endpoints, devices, user groups, or organizational units to ensure consistent protection and compliance. Develops dashboards, reporting queries, and advanced analytics across security platforms to assess user behavior, data flow, policy effectiveness, and system performance. Maintains integrations between security solutions and enterprise systems such as Security Information and Event Management, identity platforms, or network infrastructure to ensure seamless interoperability, event visibility, and unified policy enforcement. Applies updates, patches, and upgrades to security platforms, validating and documenting changes to ensure stability and continuity of operations.
15%	Develops, implements, and reviews network and security policies, standards, and procedures applicable across all security platforms. Enforces user access controls and authentication mechanisms appropriate to the organization's evolving security architecture. Conducts training sessions for IT staff and end users on network security concepts, platform capabilities, and organizational best practices. Identifies skill gaps within the team and coordinates training on new technologies, tools, and security protocols. Prepares and delivers security metrics, compliance reports, and management briefings. Documents configuration standards, migration procedures, recovery plans, and change control actions to support consistent and compliant operations. Ensures all governance activities adhere to applicable State Administrative Manual, Department Operations Manual, and departmental security requirements. Maintains version control of network and security hardware systems and special purpose vendor-supplied application software and licenses. Provides second-level support to IT field staff on complex issues.
10%	Responds to network security incidents including suspicious activity, unauthorized access, data leakage indicators, or platform alerts. Investigates incidents across various security tools, determines root causes, and recommends corrective actions. Coordinates troubleshooting efforts with infrastructure, network, and application teams to restore secure operations efficiently. Provides expert level support during urgent or afterhours production incidents and contributes to documentation of disruptions and corrective plans. Supports operational activities required to maintain a stable and secure enterprise environment.
5%	Performs other job-related duties as required.

KNOWLEDGE AND ABILITIES

Knowledge of: Information technology governance principles and guidelines to support decision making; complex and mission critical business processes and systems; principles, methods and procedures for designing, developing, optimizing, and integrating systems in accordance with best practices; system specifications design, documentation, and implementation methodologies and techniques.

Emerging technologies and their applications to business processes; business or systems process analysis, design, testing, and implementation techniques; techniques for assessing skills and education needs to support training, planning and development; business continuity and technology recovery principles and processes; principles and practices related to the design and implementation of information technology systems; information technology systems and data auditing; the Department's security and risk management policies, requirements, and acceptable level of risk; application and implementation of information systems to meet organizational requirements; project management lifecycle including the state of California project management standards, methodologies, tools, and processes; software quality assurance and quality control principles, methods, tools, and techniques; research and information technology best practice methods and processes to identify current and emerging trends in technology and risk management processes; and State and federal privacy laws, policies, and standards.

Ability to: Formulate and recommend policies and procedures; perform effectively in a fast-paced environment with constantly changing priorities; establish and maintain project priorities; apply federal, State, Department, and organizational policies and procedures to state information technology operations; apply systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems; positively influence others to achieve results that are in the best interests of the organization; consider the business implications of the technology to the current and future business environment; communicate change impacts and change activities through various methods; conduct end-user training; collaborate closely with technical subject matter experts such as database administrators, network engineers, and server administrators to ensure systems are secure and meet compliance requirements; assess situation to determine the importance, urgency, and risks to the project and the organization; make decisions that are timely and in the best interests of the organization; provide quality and timely ad hoc project information to executives, project team members, and stakeholders; develop decision-making documents; and assess and understand complex business processes and customer requirements to ensure new technologies, architectures, and security products will meet their needs.

Recognize and apply technology trends and industry best practices; assess training needs related to the application of technology; interpret audit findings and results; implement information assurance principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data; apply principles and methods for planning or managing the implementation, update, or integration of information systems components; apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality, human resources, communications, and risk and procurement management; monitor and evaluate the effectiveness of the applied change management activities; keep informed on technology trends and industry best practices and recommend appropriate solutions; foster a team environment through leadership and conflict management; effectively negotiate with project stakeholders, suppliers, or sponsors to achieve project objectives; and analyze the effectiveness of the backup and recovery of data, programs, and services.

DESIRABLE QUALIFICATIONS

Knowledge of: Cisco Enterprise products including switches, routers, intrusion detection appliances, firewalls, wireless LAN controllers and access points; Zero Trust Network security providers including Netskope and Illumio. IT systems (software) Operating Systems and (hardware) equipment; recognize its capabilities and interfaces between software and hardware.

Ability to: Write complex programs; develop detailed program specifications; analyze data and situations, reason logically and creatively, identify problems, draw valid conclusions, and develop effective solutions; apply creative thinking in the design and development of methods of processing information with information technology systems; establish and maintain cooperative relationships with those contacted in the course of the work; communicate effectively; prepare effective reports; coordinate the activities of technical personnel; prioritize work and execute on critical tasks, perform effectively under pressure and lead by example and respect of others. Work with California Department of Technology (CDT) to address any hardware device IP/ cabling and/or equipment installation, updates and/or failures as needed. Maintain/Update existing Hardware Device and Software installation/configuration Detailed Design Deliverables.

Skills: Ability to lead by example and gain the respect of others.

OTHER DOMAINS

Domain Name: System Engineering

Knowledge of: Experience in monitoring the application environments (operating system to the hardware). Including stability, performance and capacity, requirements.

Ability to: Advice, create or participate in the design of new system architecture, standards, and methods to support organizational needs. Conduct research and perform analysis to recommend system upgrades, cost-effective solutions, and process improvements to meet current and future needs. Consult with stakeholders to identify infrastructure system requirements and recommend technology, hardware, software, and plans installation. Coordinate system installation, operations, maintenance, repairs, and/or upgrades. Execute test plans for system upgrades or releases. Troubleshoot, track, and conduct root cause analysis of system/ operational issues utilizing standard procedures until resolved or escalated.

SPECIAL REQUIREMENTS OR CONTINUING EDUCATION REQUIREMENT

- CCHCS does not recognize hostages for bargaining purposes. CCHCS and CDCR have a “NO HOSTAGE” policy and all incarcerated patients, visitors, nonemployees, and employees shall be made aware of this.

SPECIAL PHYSICAL CHARACTERISTICS

Persons appointed to this position may be reasonably expected to exert up to 10 pounds of force occasionally and/or a negligible amount of force frequently or constantly to lift, carry, push, pull, or otherwise move objects. Involves sitting most of the time, but may involve walking or standing for brief periods of time.

SPECIAL PERSONAL CHARACTERISTICS

- Influence change and strengthen the community. Set an example each day through positive and pro-social role modeling, utilizing dynamic security concepts.
- Willingness to play a significant role in the collaborative efforts toward rehabilitation and public safety enhancement.
- Ability to facilitate conversations as a coach and mentor, engaging in a respectful and understanding manner.

	• Ability to build trust, improve communication, and assist with the transformation of correctional culture.

SUPERVISOR'S STATEMENT: ***I HAVE DISCUSSED THE DUTIES OF THE POSITION WITH THE EMPLOYEE***		
SUPERVISOR'S NAME (Print)	SUPERVISOR'S SIGNATURE	DATE
EMPLOYEE'S STATEMENT: ***I HAVE DISCUSSED WITH MY SUPERVISOR THE DUTIES OF THE POSITION AND HAVE RECEIVED A COPY OF THE DUTY STATEMENT***		
The statements contained in this duty statement reflect general details as necessary to describe the principal functions of this job. It should not be considered an all-inclusive listing of work requirements. Individuals may perform other duties as assigned, including work in other functional areas to cover absence of relief, to equalize peak work periods or otherwise balance the workload.		
EMPLOYEE'S NAME (Print)	EMPLOYEE'S SIGNATURE	DATE