

DUTY STATEMENT

CDCR INSTITUTION OR DEPARTMENT California Correctional Health Care Services		POSITION NUMBER (Agency – Unit – Class – Serial) 042-130-1404-973				
UNIT NAME AND CITY LOCATED Information Technology Services Division, Information Security Office – Elk Grove, CA		CLASSIFICATION TITLE Information Technology Supervisor II				
		WORKING TITLE Disaster Recovery Event and Incident Report Supervisor				
		COI Yes ☒ No ☐	WORK WEEK GROUP E	CBID S01	TENURE LT	TIME BASE FT
SCHEDULE (Telework may be available): ____ AM to ____ PM. (Approximate only for FLSA exempt classifications)		SPECIFIC LOCATION ASSIGNED TO 8280 Long Leaf 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 Chief Information Security Officer/Information Technology Manager I, the Information Technology (IT) Supervisor II serves as the Disaster Recovery, Event and Incident Report Supervisor and has significant responsibility for providing direction and oversight related to the Information Security Office. The supervisor is responsible for the indirect management and oversight of the Department's information security program ensuring protection of California Correctional Health Care Services (CCHCS) information assets and compliance with State information security policies, standards, and procedures. The supervisor has authority for formulating, recommending, and implementing information security policies, principles, and guidelines that help to ensure the integrity, confidentiality, reliability, and appropriate use of the Department's information assets in coordination with team members from the Office of Information Security and the Chief Information Security Officer. The incumbent must maintain confidentiality of information acquired while performing job duties, demonstrate ethical behavior and work cooperatively with others. Travel to institutions and after-hours support 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
25%	Provides oversight and supervision of staff responsible for implementation of security-related practices to ensure department-wide adherence to security policies, standards and procedures. Provides oversight and supervision of staff responsible for conducting risk analysis to identify critical assets, vulnerabilities, and the adequacy of security safeguards. Provides strategic direction and guidance for the CCHCS information security program. Participates in information technology planning activities as required to ensure the integration of appropriate information security protocols and practices in proposed, new, or enhanced information technology systems. Reviews Feasibility Study Reports, Project Plans, and works closely with the Enterprise Architecture team as well as the Security Operations Team to ensure appropriate security protocols are being addressed. Reviews and recommends changes to procedures dealing with confidential and sensitive data.
20%	Reviews, formulates, and recommends information security policies and principles that will ensure the integrity, confidentiality, reliability, and appropriate use of the Department's information assets. Provides guidelines to strengthen the departmental security programs to protect its information assets. Ensures the Department's goals, policies and principles function at the State level, including the legislative process, in addition to the Health Insurance Portability and Accountability Act security guidelines. Advises and assists CCHCS management through formal recommendations/risk assessments relative to the safeguarding and appropriate use of information resources. Works with the Chief Information security officer and Chief Privacy officer on the development of security standards related to IT usage
20%	Monitors threats and incidents impacting the Department's IT resources. Determines the authenticity of reported security violations and reviews all Security Incident Reports. Provides required incident reports to CCHCS management for approval, and then to State Control Agencies. Aids on issues related to physical and electronic terrorism, including emergency preparedness, response, and prevention. Collaborates with program areas to identify mission-critical systems and data and ensure the recoverability of critical business process and information systems through the development, implementation, and maintenance of an Operations Recovery Plan. Serves as an alternate member of the IT Change Control Board and as an alternate member of appropriate IT Governance Committees.
10%	Collaborates with various programs, including the CCHCS Office of Legal Affairs CCHCS Privacy Office, ITSD Security Operations and the Internal Audit Program, to ensure that CCHCS staff and management comply with the information security practices and programs. The Deputy ISO also works with CCHCS Chief Information Security Officer as well as the CDCR Office of Information Security as part of an organization Information Security Team; assists on issues related to disaster recovery, Operation Business Recovery Plans, emergency preparedness, response, and prevention.
10%	Oversees the Information Security Office staff on educating departmental staff on IT-related security and on their roles and responsibilities relative to information security and operations recovery. Develops and maintains security and privacy protection educational materials, and researches educational materials to recommend for purchase. Oversees Information Security Office staff providing security educational sessions for CCHCS staff and management. Assists with the agency-wide Security Education and Awareness programs. Oversees the development of information security policies and principles that will be applied across the department
10%	Represents the Department in statewide information security initiatives. Analyzes legislation and Federal/State mandates to determine effect on CCHCS security policies. Effectively ensures the timely coordination of all departmental and Control Agency reports related to areas of

5%	responsibility. Keeps abreast of evolving information and security technologies to ensure appropriate security controls are maintained and balanced with meeting business requirements. Assesses training needs, develops and implements training plans, and conducts annual performance evaluations; identifies and resolves staff performance issues. Recruits, develops, and retains a competent professional staff that assures an adequate level of specialized technical expertise to support current and future CCHCS' IT needs. Performs other related duties as required. Travels to assigned institutions due to operational needs.
	KNOWLEDGE AND ABILITIES <i>Knowledge of:</i> Information technology concepts, practices, and principles to provide a foundation for technology related work. Principles, techniques, and procedures related to the delivery of information technology services; the System Development Lifecycle including the associated methodologies, tools, and processes; the organization's business processes and procedures; education tools and techniques; performance monitoring tools and techniques; and data administration techniques and best practices. 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. The principles of personnel management, supervision, and training; the organization's mission, policies, principles and practices; business and management principles involved in strategic planning, resource allocation, leadership technique, coordination of people and resources; principles and practices of organization, administration, personnel (recruitment, selection, training, compensation, benefits, labor relations, negotiation, and personnel information systems), and budget management; organizational roles and responsibilities and the ability to tailor training appropriately; principles and practices of employee supervision, development, and training; a supervisor's responsibility for promoting equal opportunity in hiring and employee development and promotion; maintaining a work environment which is free of discrimination and harassment; principles of personnel management, supervision, and training; the department's Equal Employment Opportunity objectives; and a supervisor's role in Equal Employment Opportunity and the processes available to meet equal employment objectives. <i>Ability to:</i> Perform research and data gathering; analyze information and evaluate results to choose the best solution and solve problems; communicate effectively verbally and in writing as appropriate for the needs of the audience; utilize reporting tools to develop and analyze statistical reports; interpret and explain technical information to non-technical individuals; interpret customer requests to meet service needs and resolve problems; provide customer service; work cooperatively with staff at all levels; proficiently use computers and productivity software; and understand and align technology proposals with business needs. Use initiative; act independently with flexibility and tact; use logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems; perform technical analysis of proposed technology solutions; comprehend technical documents to interpret specifications, system implementations, capabilities, interdependencies, and compatibilities; serve as a technical liaison; develop and effectively utilize all available resources; develop end-user training materials; and gather data to perform statistical analysis and report outcomes.

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 which 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.

Supervise technical personnel; plan, administer, and monitor expenditures; assess, analyze, and identify information technology policy needs; establish cooperative relationships and gain support of key individuals to accomplish goals; plan, coordinate, and direct the activities of multi-disciplinary staff; effectively promote equal opportunity in employment and maintain a work environment that is free of discrimination and harassment; and effectively contribute to the department's Equal Employment Opportunity objectives.

DESIRABLE QUALIFICATIONS

Knowledge of: Analytical procedures and methods; the functions of California State Government, including the principles, practices, and policies of the California Office of Information Security and Privacy Protection; the development of security policies and procedures, security awareness programs, business continuity, disaster recovery plans, and operational recovery plans. Knowledge of the National Institute of Standards and Technology (NIST) 800-53 framework.

Ability to: Effectively communicate, both verbally and in writing, across all levels of management and the user community; develop clear, accurate, concise reports, correspondence, issue papers, memorandums, and other types of written communication to document security concerns and decisions; present such reports before IT management; network and interface effectively with business and technical personnel and communicate clearly to groups with multiple levels of IT knowledge; demonstrate strong interpersonal skills; provide technical guidance for lower-level staff and State contractors/consultants; and apply technical knowledge effectively.

Additional Qualifications: Demonstrated ability to act independently with flexibility and tact; Attainment of one or more of the reputable certifications, (i.e., Certified Information Systems Security Professional [CISSP], Microsoft Certified Systems Administrator [MCSA], Security+, Certified Information Systems Auditor [CISA], Certified Internal Auditor [CIA]).

OTHER DOMAINS

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 20 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>I HAVE DISCUSSED THE DUTIES OF THE POSITION WITH THE EMPLOYEE</i>		
SUPERVISOR'S NAME (Print)	SUPERVISOR'S SIGNATURE	DATE
EMPLOYEE'S STATEMENT: <i>I HAVE DISCUSSED WITH MY SUPERVISOR THE DUTIES OF THE POSITION AND HAVE RECEIVED A COPY OF THE DUTY STATEMENT</i>		
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