

DUTY STATEMENT

RPA

EFFECTIVE DATE:

CDCR INSTITUTION OR DEPARTMENT California Correctional Health Care Services (CCHCS)	POSITION NUMBER (Agency – Unit – Class – Serial) 042-130-1312-054
UNIT NAME AND CITY LOCATED CCHCS Information Technology Services Division, Information Security Office - Sacramento	CLASS TITLE Staff Information Systems Analyst (Spec)
WORKING DAYS AND WORKING HOURS 8:00 a.m. to 5:00 p.m. (Approximate only for FLSA exempt classifications)	SPECIFIC LOCATION ASSIGNED TO
PROPOSED INCUMBENT (if known)	CURRENT POSITION NUMBER (Agency – Unit – Class – Serial)

YOU ARE A VALUED MEMBER OF THE DEPARTMENT'S TEAM. YOU ARE EXPECTED TO WORK COOPERATIVELY WITH TEAM MEMBERS AND OTHERS TO ENABLE THE DEPARTMENT TO PROVIDE THE HIGHEST LEVEL OF SERVICE POSSIBLE. YOUR CREATIVITY AND INGENUITY ARE ENCOURAGED. YOUR EFFORTS TO TREAT OTHERS FAIRLY, HONESTLY AND WITH RESPECT ARE CRITICAL TO THE SUCCESS OF THE DEPARTMENT'S MISSION.

Under general direction of the Data Processing Manager III, the Staff Information Systems Analyst (Spec) works as a technical specialist to lead the infrastructure security tasks for the Information Security Office (ISO). The ISO mission is to ensure a secure computing environment that will provide availability, confidentiality and integrity of information. The CCHCS must comply with federal and state security regulations including *National Institute of Standards and Technology (NIST)* Security requirements, HIPAA Security Rule, and *State Administrative Manual (SAM)* Information Security Sections. The CCHCS ISO is committed to adopting the best practices of information security industry as promulgated by the private, state and federal entities in order to secure protected health information (PHI), to counteract hacker attacks, and to protect against virus infection throughout the organization.

% 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

30%	Oversee the security of the client-server infrastructure of the CCHCS by ensuring that the following activities are performed by appropriate IT personnel: implement: Enterprise Anti-virus/malware, develop Server security standards and a Server hardening guide, develop a Client security standards and a Client hardening guide, develop Active Directory (AD) security standards and AD hardening guide. Participate in the development of the hardening security standards for servers by working with other CCHCS and California Department of Corrections and Rehabilitation design and support teams. Produce an infrastructure security event analysis solution that details how infrastructure components can be integrated into the enterprise security event management (SEM) and correlation engine to log activity and identify incidents. Investigate and report on client and server security incidents by following the department and state required procedures and completing the required documentation. Participate in an overall incident management team and address incident response related activities as they pertain to client-server systems by assisting the incident team in security incident identification, containment, eradication, recovery, and reporting efforts.
20%	Perform regular client-server infrastructure vulnerability and risk assessments of various automated systems by identifying areas of risk, quantifying or ranking the risk, providing a recommended risk treatment plan, and calculates estimates for the necessary people, process, and technology to remediate identified risk. Ensure that the risk and vulnerability

	<p>assessments take into account any PHI in transit and at rest by identifying where all PHI is located in the department. Assess the data exchange activities with external entities and other systems by understanding the nature of the data and the necessity for the exchange. Evaluate the controls that are present at the application layer which are an important component of the infrastructure security over data and databases by applying state and national standards that have been established for application controls. Assess the vulnerabilities and risks related to the System Development Life Cycle by verifying that the appropriate security controls related to the acquisition, development and maintenance of information systems are being used. Incorporate the infrastructure vulnerability and risk assessments into the overarching enterprise vulnerability assessments by including the workstations and network controls for the whole enterprise.</p>
20%	<p>Develop a list of infrastructure security requirements for client-server related projects that will be integrated into the overarching CCHCS information security requirements document. Incorporate security industry standards and controls. Ensure that the infrastructure security requirements include security controls for name resolution server, AD, group policies, file and print services, system management and monitoring services, and security patch management systems. Verify that the infrastructure security requirements comply with all applicable legal and regulatory requirements and adhere to industry standards and best practices by constructing a security matrix and mapping document.</p>
10%	<p>Produce a client-server Infrastructure Security Architecture document by detailing all applicable legal, regulatory and statutory infrastructure security requirements, secure internal and external name resolution design, systems deployment, security patch management, AD and Group Policy Object GPO design, and systems management and monitoring. Integrate the infrastructure security architecture into the enterprise information security architecture by understanding the business strategies and aligning infrastructure security with these strategies.</p>
10%	<p>Participate in the development of information security policies and procedures that are in compliance with the appropriate state and federal security regulations that impact the CCHCS as a provider of medical, dental and mental health services to inmates. Develop the policies and procedures by using security industry best practices and authoritative sources.</p>
5%	<p>Participate in the contingency planning for the CCHCS by completing assignments related to the development of the Emergency Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. Prepare the contingency planning documents by following the state guidelines and regulations.</p>
5%	<p>Perform other related tasks as required.</p>

DUTY STATEMENT

% 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. <i>(Use addition sheet if necessary)</i>	
	<p>KNOWLEDGE AND ABILITIES</p> <p><i>Knowledge of:</i> Principles of public administration, organization, and management; information technology systems equipment, software, and practices; analytical techniques; technical report writing.</p> <p><i>Ability to:</i> Analyze information and situations, identify and solve problems, reason logically, and draw valid conclusions; develop effective solutions; apply creative thinking in the design of methods of processing information with information technology systems; monitor and resolve problems with information technology systems hardware, software, and processes; establish and maintain effective working relationships with others; communicate effectively.</p> <p>DESIRABLE QUALIFICATIONS</p> <p><i>Special Personal Characteristics:</i> Effective communication skills, both written and verbal.</p> <p><i>Interpersonal Skills:</i> Ability to influence and motivate individuals and teams working toward mutual goals which have basic cooperative attitudes.</p> <p><i>Additional Desirable Qualifications:</i> Experience including but not limited to identifying infrastructure based vulnerabilities, designing infrastructure based threat countermeasures, participating in infrastructure related incident management activities, and managing infrastructure related risk; Experience working on large and complex infrastructure security or infrastructure related IT projects; Experience working on infrastructure security compliance activities in a regulated industry; Experience performing infrastructure security related activities in the healthcare industry; Experience providing infrastructure security or network related IT related consulting services to clients in the public and/or private sector(s); Knowledge of state IT policy and governance processes; Knowledge of state IT policy and governance processes; Experience performing infrastructure risk assessments; Experience performing infrastructure vulnerability assessments; Experience designing, implementing, and managing infrastructure based technical controls; Experience working in an environment where network security services are provided by an external service provider; Experience participating in enterprise infrastructure design and implementation efforts with a focus on integrating security into the enterprise design; Certified in information security [Certified Information Systems (CIS) Security Professional, CIS Manager, or CIS Auditor]; SysAdmin, Audit, Network, Security Institute (SANS) Certified; Understanding of State governance process; Experience with projects supporting correctional environments and processes.</p> <p>SPECIAL PHYSICAL CHARACTERISTICS</p> <p>Incumbent occasionally moves equipment either solely (40 lbs. max.) or with another person (100 lbs. max.), may be required to open equipment and replace parts as directed, and is expected to exert up to 40lbs of force occasionally and/or a negligible amount of force frequently or constantly to lift, carry, push, pull, or otherwise move objects. Involves frequent walking, standing and sitting. Persons appointed to this position must be able to travel to assigned locations.</p>	
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