

SHADED AREA TO REFLECT RECLASS POSITION NUMBER ONLY**DUTY STATEMENT**

RPA

EFFECTIVE DATE:

10/26/2016

CDCR INSTITUTION OR DEPARTMENT Enterprise Information Systems (EIS)	POSITION NUMBER (Agency – Unit – Class – Serial) 065-620-1558-500
UNIT NAME AND CITY LOCATED Aerojet, Sacramento	CLASS TITLE System Software Specialist II (Tech) Sup
WORKING DAYS AND WORKING HOURS 8:00 a.m. to 5:00 p.m. (Approximate only for FLSA exempt classifications)	SPECIFIC LOCATION ASSIGNED TO Information Security Office (ISO)
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 IV, the System Software Specialist II (Tech) Supervisor will act as the supervisor over staff within the agency Information Security Office (ISO). The group is responsible for the CDCR's most complex information security functions. The CDCR must comply with federal and state security regulations including NIST Security requirements, HIPAA Security Rule, and SAM Information Security Sections. The Agency 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 confidential and sensitive information, to counteract hacker attacks, and to protect against virus infection throughout the organization. The ISO mission is to ensure a secure computing environment that will provide availability, confidentiality and integrity of information.	
% 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>
ESSENTIAL FUNCTIONS	
30%	<p>Supervise and provide technical oversight of policy administration for the information security appliance suite used to manage the CDCR network assets. This would include the providing technical guidance to ISO staff as well as guidance on technical integration, process development, improvement, tuning, maintenance, and support of:</p> <ol style="list-style-type: none"> 1. Endpoint/host security to include anti-malware, encryption, host intrusion detection, host data loss prevention and change management; 2. Security incident and event monitoring; 3. Perimeter security to include proxy policy, firewall access control lists, and special access requests; 4. Network security to include network data loss prevention and network intrusion prevention; and 5. Vulnerability management to include scanning, validation, remediation, and testing. <p>The incumbent is responsible for engineering security policies that mitigate and minimize the risk to CDCR information assets while ensuring that business process functionality is not hindered.</p>
20%	<p>Supervise and lead security monitoring of assets on the CDCR network. This would include providing guidance on identifying potential security events, communicating with various units through the organization to resolve potential issues, and utilizing network software and hardware security tools/appliances to identify potential threats and vulnerabilities. The incumbent will also serve as the lead member of the Computer Security Incident Response Team (CSIRT) by providing technical analysis and identifying potential remediation procedures.</p>

DUTY STATEMENT

RPA

EFFECTIVE DATE:
10/26/2016

20%	Perform and lead the ISO unit in complex technical vulnerability and risk assessments of the CDCR network managed assets including the network hardware components, network schematics for enterprise applications, network endpoints (workstations and servers), distributed locations remote access, and data center operations and facilities by using vulnerability tools. Lead the development and implementation of a network risk assessment methodology that includes the selection and application of vulnerability and countermeasure tools, identification of threats to the network, assessment of risks associated with threats, and recommendations for corrective actions by applying security industry standards such as NIST, SANS, and COBIT. The position will lead the unit to assess threats associated with all areas technologies that communicate over the CDCR network resources. This would include such technologies as wireless (WiFi), laptops and mobile workstations, smart phones, email communications, VPN/Remote access, storage capacity, backup processes, internal and external system interfaces, third party applications, web proxy, and external contractor activities.
10%	Supervise and provide technical guidance of CDCR's contracted information security services to ensure that tactical or strategic efforts of the ISO are being properly supported by meeting with the contractors on a regular basis. Ensure that the CDCR security contract components are being properly communicated, implemented, and managed through the use of management status reports. Ensure that regular information security service status reports are communicated to the CDCR ISO including, but are not limited to, action items completed, planned action items, network risks, operational issues, incident escalations, and Service Level Agreement (SLA) performance metrics. Perform oversight of the security contractor to ensure compliance with regulatory requirements and internal procedures and guidelines.
10%	Provide technical consultation on IT projects that are being proposed that will involve the CDCR network while identifying the impact of the project on the overall CDCR infrastructure by interpreting business requirements and detailed design documents. Apply the advanced knowledge of network security to identify risks relevant to the project and CDCR enterprise network. Ensure IT projects comply with the applicable state and federal regulatory information security requirements.
5%	Participate in the development of information security policies and procedures for the ISO by applying security industry best practices, state and federal mandates, health and medical related security standards and other authoritative sources. Write the security policies and procedures in order to ensure 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 by being knowledgeable of security industry references such as NIST, SANS, ISO.
5%	Perform network related tasks as required.

KNOWLEDGE AND ABILITIES

Knowledge of: Principles of public administration, organization, and management; information technology systems equipment, software, and practices; analytical techniques; technical report writing and principles of personnel management, supervision, and training; the department's Equal Employment Opportunity objectives; a manager's role in the Equal Employment Opportunity and the processes available to meet equal employment objectives.

Ability to: 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 and supervise technical personnel; effectively contribute to the department's equal employment objectives.

DESIRABLE QUALIFICATIONS

Special Personal Characteristics: Effective communication skills, both written and verbal.

DUTY STATEMENT

RPA

EFFECTIVE DATE:

10/26/2016

Interpersonal Skills: Ability to influence and motivate individuals and teams working toward mutual goals which have basic cooperative attitudes.

1. *Additional Desirable Qualifications:* Experience including but not limited to identifying network based vulnerabilities, designing network based threat countermeasures, participating in network related incident management activities, and managing network related risk; Experience working on large and complex network security or network related IT projects; Experience working with Cisco related network security solutions; Experience working on network security compliance activities in a regulated industry; Experience performing network security related activities in the healthcare industry; Experience providing network 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 network risk assessments; Experience performing network vulnerability assessments; Experience designing, implementing, and managing network based technical controls including but not limited to Cisco Adaptive Security Appliance (ASA) firewalls, Cisco Firewall Software Module (FWSM), Cisco network based Intrusion Prevention Systems (IPS), and Cisco based secure remote access solutions; Experience working in an environment where network security services are provided by an external service provider; Experience participating in enterprise network design and implementation efforts with a focus on integrating security into the enterprise design; Certified in Cisco Security (CCSP, CCNP Security, or CCIE Security); Certified in information security (CISSP, CISM, or CISA); SANS Certified; Understanding of State governance process; Experience with projects supporting correctional environments and processes. Knowledge of the OSI model; Knowledge of State Information Security policies and structure. Ability to interpret various software code written in language including, but not limited to binary, machine, assembly, various programming languages and object based programming. Experience or knowledge of information security incident response process including, but not limited to forensic analysis and preservation of evidence.

SPECIAL PHYSICAL CHARACTERISTICS

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.

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