

ENTERPRISE INFORMATION SERVICES DUTY STATEMENT

Section	Information Security and Change Management
Unit	Information Security
Position Number	065-649-1587-001
Classification	Systems Software Specialist I (Technical)
Revised Date	8/4/2016

Supervision: Under the general supervision of the Data Processing Manager II, the Systems Software Specialist I (Technical) (SSS I Tech.) will work as a security technical specialist for the Agency Information Security Office (AISO) to contribute with the design, implementation, and monitoring of the information security for the Career Technical Education (CTE) Basic Project and other projects in designing, implementing, and monitoring the Inmate Ward Secure Network. The California Department of Corrections and Rehabilitation (CDCR) must comply with Federal and State security regulations. The SSS I Tech. will be 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 malware infection throughout the organization. The mission is to ensure a secure computing environment that will provide availability, confidentiality, and integrity of information.

The SSS I Tech. will work within AISO which is comprised of security analysts and specialists performing a wide array of complex security related tasks. This position will provide technical security expertise to and collaborate with other units in security related areas within EIS and the Division of Rehabilitative Programs (DRP).

Knowledge/Skills/Abilities: The SSS I Tech. must have the ability to solve complex business problems and possess interpersonal communication skills. The incumbent must also be knowledgeable regarding principles of public administration, organization, and management; information technology systems hardware, software, and industry practices. The incumbent must also be familiar with analytical techniques; and technical report writing.

Specific technical knowledge includes:

- Layered security principles, including network segmentation, perimeter security, database security, end point security, and event monitoring.
- System and application security threats and vulnerabilities.
- Basic system administration principles.
- Network and operating system hardening techniques.
- N-Tiered platform architecture.
- Different classes of attacks (e.g., passive, active, insider, close-in, or distribution).
- General attack stages (e.g., foot printing and scanning, enumeration, infiltration, escalation of privileges, maintaining access, network exploitation, data exfiltration, and covering tracks).
- Familiarity with configuration monitoring and support of wireless network infrastructure security components.

Guidelines: The SSS I Tech. will be responsible for participating as an expert within a team of information systems analysts and system software specialists at the journey levels.

ENTERPRISE INFORMATION SERVICES DUTY STATEMENT

Scope and Effect: As the security technical specialist on the development, implementation, and monitoring of complex IT projects, the SSS I Tech. will be responsible for reviewing appropriate levels of security protocols and procedures, designing, and placing security controls and monitoring in place, and performing appropriate risk management for threats and vulnerabilities. The incumbent will be required to demonstrate in-depth technical knowledge of security controls, testing and assessment methodologies. The incumbent must also possess a solid, end-to-end understanding of CDCR's corresponding business processes, policies, and procedures. The incumbent will be responsible for assisting business process owners, administrators, and the client community in timely resolution of incidents. The incumbent will be required to operate a personal computer daily for extended periods of time. Excellent communication skills, both written and verbal, are expected of the SSS I Tech. while executing duties.

This position requires occasional overtime and traveling.

Types and Level of Contacts: The incumbent will devote time to customer service and public relations. On-going contacts will be made with all levels of management. Within CDCR, contacts are made with EIS management and administrative staff, and staff from DRP and other offices and divisions of the Department. Outside of CDCR, contacts are with consultants/contractors, industry representatives, professional/planning groups, private/public utility representatives, product vendors, and Control Agencies such as the State Controller's Office, Department of Technology Services (DTS), and Department of General Services. Issues discussed with contacts may include those involving: security threats, vulnerabilities, and incidents, policies, standards, protocols, emerging technologies, tools, and other areas.

The actual duties of the SSS I Tech. include, but are not limited to, the following:

50%	Information Security Testing, Monitoring, and Auditing
	<ul style="list-style-type: none">• Conduct security assessments to identify vulnerabilities and risks.• Document security assessment and testing results.• Review security assessments to track the organization's compliance with policies and requirements.• Recommend security controls to mitigate identified security vulnerabilities and risks.• Conduct impact analyses to determine the security impact of pending changes to the enterprise architecture resulting from the addition or removal of information systems.• Active and passive security event monitoring.• Configuration monitoring and support of wireless network infrastructure security components.
15%	Information Security Incident Management
	<ul style="list-style-type: none">• Respond to potential security incidents.• Conduct advanced root-cause analyses to identify or resolve issues that cause a significant impact to the CDCR environment.• Respond and mitigate malware activity, potential data breaches, unauthorized access events, Denial of Service (DoS) attacks, and phishing attacks.• Perform incident handling tasks using cybersecurity tools to support deployable Incident Response Teams.

ENTERPRISE INFORMATION SERVICES DUTY STATEMENT

15%	Information Security Risk Management
------------	---

- Document, review, and implement security controls within the information system and its environment of operation.
- Ensure appropriate use of assessment procedures.
- Monitor the security controls within information system.
- Participate in complex risk assessments on IT projects that may involve the CDCR secured network.
- Perform complex technical vulnerability assessments by using vulnerability tools.
- Assess threats associated with technologies and processes used within the CDCR environment. This includes, but is not limited to, such technologies as wireless (Wi-Fi), laptops and mobile workstations, smart phones, email communications, VPN/Remote access, storage capacity, back-up processes, internal and external system interfaces, third party applications, web proxy, and external contractor activities.

10%	Information Security Operations
------------	--

- Install, configure, integrate and maintain service contracts, hardware, and software to support the security policies and business practices of the organization.
- Report information security service statuses to team leads and managers.
- Review and disseminate security intelligence as appropriate.
- Test and ensure security measures are effective in their purpose and recommend adaptations as necessary.
- Investigate possible security incidents and report as appropriate.
- Evaluate and assess application or system to ensure compliance with Federal, State, and other regulatory requirements.
- Scan network sites to identify potential vulnerabilities and inform owners of risks, mitigation strategy, or corrective actions.

5%	Information Security Engineering and Architecture
-----------	--

- Participate with the Information Security Architecture process.
- Provide analysis of business impact, risk, and vulnerabilities of the Security Architecture standards.
- Research and maintain knowledge of current and emerging technologies, trends, best practices, and State directives.
- Develop and ensure security solutions and technical artifacts are in place to mitigate identified risks, meet business objectives, and comply with regulatory requirements.
- Serve as a security subject matter expert to ensure projects comply with enterprise IT security policies, industry regulations, and best practices.
- Evaluate and analyze the Department's information assets to ensure security controls provide appropriate controls: Application portioning, denial of service protection, boundary protection, confidentiality of transmitted information and cryptographic protection.

5%	Information Security Policies and Procedures
-----------	---

- Under direction, develop, disseminate, and update information security policies and procedures.
- Develop and/or review data sharing agreements prior to the release of classified information to ensure compliance and privacy of personal information.
- Perform data classification and implementing appropriate security control policies.

**ENTERPRISE INFORMATION SERVICES
DUTY STATEMENT**

- Perform other related tasks as required and other duties as assigned.

Employee: _____

Date: _____

Immediate Supervisor: _____

Date: _____