

## ENTERPRISE INFORMATION SERVICES DUTY STATEMENT

<b>Section</b>	Information Security and Change Management
<b>Unit</b>	Information Security
<b>Position Number</b>	065-649-1373-004
<b>Classification</b>	Systems Software Specialist II (Technical)
<b>Revised Date</b>	8/4/2016

**Supervision:** Under the general supervision of the Data Processing Manager IV, Information Security Officer (ISO), the Systems Software Specialist II (Technical) (SSS II Tech.) will work as the technical specialist for the Agency Information Security Office (AISO) to lead the information security efforts 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 rules and regulations. The SSS II 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 II Tech. will work within the AISO which is comprised of security analysts and specialists performing a wide array of complex security related tasks. The SSS II Tech. position will provide advanced technical advice and train staff in performing the complex technical security functions for the protection of CDCR's and other technical and operational areas. 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 II Tech. must have the ability to solve complex business problems and be able to provide leadership and process discipline to the job. Interpersonal communication and leadership skills are necessary to serve in this lead capacity. The incumbent must also have the ability to influence and motivate individuals and teams working toward mutual goals with basic cooperative attitudes. The incumbent must also be knowledgeable regarding principles of public administration, organization, and management; IT systems equipment, software, and practices; 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 II Tech. will be responsible for acting a senior level 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 information technology (IT) projects, the SSS II Tech. will be responsible for architecting 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 an 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 a 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, will be required of the SSS II 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 will be made with EIS management, administrative staff, and staff from other offices and divisions of the Department such as DRP. Outside of CDCR, the incumbent will have contact with consultants/contractors, industry representatives, professional/planning groups, private/public utility representatives, product vendors, and Control Agencies such as the State Controller's Office (SCO), Department of Technology Services (DTS), and Department of General Services (DGS). 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 II Tech. include, but are not limited to, the following:

<b>25%</b>	<b>Information Security Risk Management</b>
	<ul style="list-style-type: none"><li>• Identify security controls for the information system based on the security categorization.</li><li>• Tailor and supplement controls based on an organizational assessment of risk and pertinent conditions.</li><li>• Design, architect, and document processes to implement security controls.</li><li>• Assess implemented security controls for effectiveness and appropriateness.</li><li>• Monitor security controls on an ongoing basis.</li><li>• Report security state of the system to organization.</li><li>• Perform complex risk assessments on IT projects that may involve the CDCR network.</li><li>• Perform complex technical vulnerability assessments by using vulnerability tools.</li><li>• Develop and implement a risk management methodology according to appropriate industry security standards such as NIST.</li><li>• Assess threats associated with technologies that communicate over the CDCR networked resources. This would include such technologies as wireless (Wi-Fi), 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.</li></ul>

# ENTERPRISE INFORMATION SERVICES DUTY STATEMENT

<b>25%</b>	<b>Information Security Testing and Monitoring</b>
------------	--

- Plan, develop, conduct, and review security assessments and processes 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.

<b>15%</b>	<b>Information Security Incident Management</b>
------------	---

- Respond to potential security incidents.
- Conduct advance 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.

<b>15%</b>	<b>Information Security Operations</b>
------------	--

- Install, configure, integrate, and maintain service contracts, hardware, and software to support the security policies and business practices of the organization.
- Ensure that regular information security service status reports are communicated to the CDCR AISO.
- Review, disseminate, and track security-related intelligence to determine necessary action(s).
- Test and ensure security measures are effective in their purpose.
- Monitor the secured networks for anomalous activities and respond appropriately.
- Investigate possible security incidents and report as appropriate.
- Evaluate and assess systems or applications to ensure compliance with Federal, State, and other regulatory requirements.
- Manage and conduct site vulnerability scans and inform owners and system custodians of risks, mitigation strategies, and/or corrective actions.

<b>15%</b>	<b>Information Security Engineering and Architecture</b>
------------	--

- 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.

## ENTERPRISE INFORMATION SERVICES DUTY STATEMENT

- 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 control provide appropriate controls: Application partitioning, denial of service protection, boundary protection, confidentiality of transmitted information and cryptographic protection.

<b>5%</b>	<b>Information Security Policies and Procedures</b>
-----------	---

- Develop, disseminate, and update information security policies and procedures.
- Develop and/or review data sharing agreements prior to release of classified information to ensure compliance and privacy of personal information.
- Perform data classification and implement appropriate security control policies.
- Perform other related tasks as required and other duties as assigned.

Employee: \_\_\_\_\_

Date: \_\_\_\_\_

Immediate Supervisor: \_\_\_\_\_

Date: \_\_\_\_\_