**OFFICE OF THE STATE CONTROLLER**

DUTY STATEMENT

|  |  |
| --- | --- |
| **EMPLOYEE NAME**  Vacant | **DIVISION**  Information Systems |
| **CLASSIFICATION TITLE**  Information Technology Supervisor II | **UNIT NAME - LOCATION**  Information Security Office - Sacramento |
| **WORKING TITLE**  Information Security Program Supervisor | **POSITION NUMBER**  051-340-1404-019 |
| **Information Technology Domain**  Information Security Engineering | **EFFECTIVE DATE**  TBD |

**SECTION A: GENERAL DESCRIPTION**

Under the general direction of the Chief Information Security Officer (CISO), an Information Technology Manager II in the Information Security Office (ISO), the incumbent acts in a lead person capacity performing a range of management and technical duties to contribute to successful operations of the State Controller’s Offices (SCO) Enterprise Information Security Program activities. Such as, providing ongoing collaboration and consultation with key partners throughout SCO. The incumbent’s role includes leading the specific functional responsibilities of your team, which involves overseeing team performance and deliverables through developing and executing of the CISO’s and SCO’s strategic vision and plan and ensuring the team’s actions align with the larger goals of the SCO. Specific duties include but are not limited to the following:

**SECTION B: ESSENTIAL FUNCTIONS**

*Candidates must have the ability to perform the following essential functions with or without reasonable accommodations*.

Percentage of

Time Spent Typical Task

|  |  |
| --- | --- |
| 40% | Provides supervision in the development and implementation of the SCO’s Enterprise Information Security Program that enables the SCO to establish consistent, effective information security practices and minimize risk. Supervises the design, implementation and evaluation of SCO’s information security standards, guidelines, recommendations, procedures, initiatives and processes to ensure ongoing maintenance of security and consistency with state and federal laws, rules, regulations and best practices.  Evaluates and reports the progress of projects through meetings and written reports to higher-level management.  Collaborates with Senior Analysts to coordinate activities and assignments of the project team with programmers, vendors, consultants, contractors, and functional managers of support, operational, and customer staff.  Establishes performance expectations; provides continuous feedback; completes appraisals and individual development plans annually; completes probation reports on a timely basis; and conducts other performance management activities, including adherence to the State’s discipline policy which may include corrective or disciplinary action.  Supervises Information Security Office assets and human resources in accordance with established policies, procedures, and labor contracts. |
| 25% | Provides supervision in the development and implementation of the SCO’s Enterprise Information Security Program’s information security risk, planning, assessment and vulnerability management initiatives and processes. Develops and maintains information security standards, procedures, initiatives and processes to address all applicable requirements throughout the life cycle of each SCO information system to ensure compliance with applicable requirements and information asset owner acceptable risk determinations. |
| 15% | In collaboration with the SCO CISO and ISO staff represents the ISO regarding information security risk management and assurance to external IT projects and auditors.  Supervises and reports on the development, installation, and maintenance of complex IT systems and projects.  Develops training plans and training material for complex changes to the SCO’s system environments, and provide technical training to ISO staff. |
| 15% | Assigns and collaborates with ISO project leads concerning division, agency, and statewide projects. For example, the CSPS, CalATERS, and FI$Cal project implementations.  Tracks project status, provide direction in changes of priorities and schedules and provide guidance or recommendations on complex system assessments.  Manages and tracks the development of written standards, policies, and procedures.  Performs project management responsibilities and activities using State and SCO project management methodology and practices. |
| 5% | Represents the CISO in meetings with theSCO management and analysts, the California Department of Technology (CDT), decentralized agencies and campuses, projects, and hardware/software vendors regarding the SCO's security and privacy standards, procedures, and requirements. |

**SECTION C: NON-ESSENTIAL FUNCTIONS**

|  |  |
| --- | --- |
| % | NONE |

**SECTION D: ADA REQUIREMENT (N/A)**

Alternative will be provided for incumbents who are unable to perform the non-essential functions of the job because of a disability as defined by the Americans with Disabilities Act.

**SECTION E: KNOWLEDGE, SKILLS AND ABILITIES**

**Knowledge**:

* Knowledge of computer networking concepts and protocols, and network security methodologies.
* Knowledge of risk management processes such as the Risk Management Framework (RMF) (e.g., methods for assessing and mitigating risk).
* Knowledge of state and federal laws, regulations, policies, guidelines and ethics as they relate to information security and privacy.
* Knowledge of information security and privacy principles. 8888
* Knowledge of physical and cyber threats and vulnerabilities.
* Knowledge of information technology (IT) architectural concepts and frameworks.
* Knowledge of the organization's core business/mission processes.
* Knowledge of compliance auditing.
* Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).
* Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL])
* Knowledge of information technology (IT) acquisition/procurement requirements.
* Knowledge of the state acquisition/procurement life cycle process.
* Knowledge of specific operational impacts of cybersecurity lapses.
* Knowledge of business continuity and disaster recovery continuity of operations plans.
* Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
* Knowledge of incident response and handling methodologies.
* Knowledge of information security program management and project management principles and techniques.
* Knowledge of an organization's information classification program and procedures for information compromise.
* Knowledge of controls related to the use, processing, storage, and transmission of data.
* Knowledge of security and privacy principles relevant to confidentiality, integrity, availability, authentication, non-repudiation and accountability.
* Knowledge of information security program management and project management principles and techniques.
* Knowledge of NIST Special Publication (SP) 800-53 and 800-53A specifications and processes.
* Knowledge of the Federal Information System Controls Audit Manual (FISCAM) methodology for auditing information system controls.
* Knowledge of the System Development Life Cycle (SDLC).
* Knowledge of information security systems engineering principles (NIST SP 800-160).
* Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI].
* Knowledge of cyber and physical security and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
* Knowledge of information asset resiliency and redundancy.
* Knowledge of cloud computing models [i.e., Public, Private, Hybrid, and Community) and services (i.e., Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)].
* Knowledge of protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
* Knowledge of configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
* Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
* Knowledge of vulnerability, configuration and penetration testing principles, tools, and techniques.
* Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs).
* Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
* Knowledge of new and emerging information technology (IT) and security technologies.
* Knowledge of privacy disclosure statements based on current State and Federal laws.
* Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects.

**Skills:**

* Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
* Skill in creating policies that reflect organizational security objectives.
* Skill in communicating with all levels of management including Executive members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
* Skill to anticipate new security threats.
* Skill to remain aware of evolving technical infrastructures.
* Skill to use critical thinking to analyze organizational patterns and relationships.
* Skill to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise.
* Skill in assessing security and privacy controls based on cybersecurity principles and tenets. (e.g., NIST SP 800-53, Cybersecurity Framework, etc.).
* Skill in conducting security and privacy capabilities and requirements analysis.
* Skill in administrative planning activities, to include preparation of functional and specific assessment and test support plans, plans, findings and gap analyses; plans of action with milestones (POAMs) and corrective action plans (CAPs), preparing and managing correspondence, and staff (desk) procedures.
* Skill in preparing asset or environment specific policies, procedures, workflows,
* Skill in preparing asset assessment certification / attestation documents.
* Skill in evaluating security assessment and test plans for applicability and completeness.
* Skill in assessing the security design of network, system or application architectures concepts including topology, protocols, components operational and physical environment designs.
* Skill in applying and incorporating information technologies into proposed solutions.
* Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.
* Skill in operating system administration (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).
* Skill in developing and executing security awareness and education training programs and curricula.
* Skill in interfacing with customers.
* Skill in talking to others to convey security awareness and education information effectively.
* Skill in utilizing feedback to improve security awareness and education processes, products, and services.
* Skill in preserving evidence integrity according to standard operating procedures or State standards.
* Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
* Skill in performing security and privacy incident damage assessments.
* Skill in maintaining RACF administration services.
* Skill in diagnosing connectivity problems.

**Ability:**

* Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, standards and guidelines in support of organizational information security activities.
* Ability to apply critical reading/thinking skills.
* Ability to exercise judgment when policies are not well-defined.
* Ability to interpret and apply laws, regulations, policies, and guidance relevant to organizational information security objectives.
* Ability to tailor technical and planning information to a customer’s level of understanding.
* Ability to prioritize and allocate information security resources correctly and efficiently.
* Ability to relate strategy, business, and technology in the context of organizational dynamics.
* Ability to understand technology, management, and leadership issues related to organization processes and problem solving.
* Ability
* Ability to ensure information security management processes are integrated with strategic and operational planning processes.
* Ability to ensure that senior officials within the organization provide information security for the information and systems that support the operations and assets under their control.
* Ability to develop asset and business administrative documents (e.g., policies, procedures, plans, reports, workflows, and topology diagrams) in compliance with laws, regulations, policies, and standards in support of the SCO’s Information Security Program.
* Ability to produce technical documentation.
* Ability to interpret and apply State and Federal laws, regulations, policies, and guidance relevant to the SCO’s Information Security Program’s security and business objectives.
* Ability to work across SCO division and business units to implement the SCO’s Information Security Program’s security and privacy principles and programs, and align security and privacy objectives with asset and business operational environments.
* Ability to relate strategy, business, and technology in the context of SCO organizational dynamics.
* Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—to leverage analytical and technical expertise.
* Ability to understand the basic concepts and issues related to security and privacy and their SCO and State organizational impact.
* Ability to interpret and translate customer requirements into operational capabilities.
* Ability to translate assessment and test data results into evaluative conclusions.
* Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.
* Ability to collaborate effectively with others.
* Ability to function effectively in a dynamic, fast-paced environment.
* Ability to develop clear directions and instructional materials.
* Ability to analyze assessment and test data.
* Ability to collect, verify, and validate assessment and test data.
* Ability to develop security awareness and education curriculum that speaks to the topic at the appropriate level for the target audience.
* Ability to communicate complex security awareness and education information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
* Ability to prepare and present briefings.
* Ability to develop clear direction and instructional materials.
* Ability to conduct training and education needs assessment.
* Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
* Ability to monitor advancements in information security and privacy technologies to ensure organizational adaptation and compliance.
* Ability to respond to after business hour (callback) physical security alarm events.

**SECTION F: RESPONSIBILITY FOR DECISIONS (CONSEQUENCE OF ERROR)**

Incumbent will administer security systems and make consultative recommendations concerning the security and privacy of SCO’s environments, including but not limited to those that pertain to all business programs, operations, projects, data, networks, systems, applications; personnel and facility physical security. The effect of this administration and consultative recommendations activities will affect efficiency and effective operation and performance of the SCO environment’s and their overall security posture. Errors in administration or recommendation judgment and decision making could result in a degradation of the SCO environment’s availability and operations, due diligence expected security posture; violation of state and federal security and privacy laws, regulations, rules, and standards, and adverse consequences to SCO’s business operations and information assets, data, mission, functions, image, or reputation.

**SECTION G: PERSONAL CONTACT**

The Incumbent will have regular contact with the SCO CISO, ISO colleagues, SCO executives, division chiefs, managers, supervisors, staff, customer, stakeholders, contractors and vendors. The Incumbent may have contact with other state agencies, federal government and local government.

**SECTION H: WORK ENVIRONMENT**

While at their base of operation, Incumbent will work in a climate-controlled office cubicle under artificial light. The office is located in “high rise” office structure. However, due to periodic problems with the heating and air conditioning, the building temperature may fluctuate. Working hours will be set sometime between 6:00 a.m. and 7:00 p.m. Monday through Friday, working before and after this time may be required, and vacations may be restricted, due to business needs. Employees may be required to travel in within Sacramento County to attend meetings and respond to afterhours physical security alarm events.

**SECTION I: PHYSICAL REQUIREMENTS**

Any lifting, moving, keying, etc. required for this position.

| Check the frequency of activity required of the employee to perform the job | | | | |
| --- | --- | --- | --- | --- |
| Activity  (Hours per day) | Never  (0 Hours) | Occasionally  (up to 3 hours) | Frequently  (3 to 6 hours) | Constantly  (6 to 8 hours) |
| Sitting |  |  |  | X |
| Walking |  | X |  |  |
| Standing |  | X |  |  |
| Bending (neck/waist) |  |  |  | X |
| Squatting |  | X |  |  |
| Climbing |  | X |  |  |
| Kneeling |  | X |  |  |
| Crawling |  | X |  |  |
| Twisting (neck/waist) |  | X |  |  |
| Is repetitive use of hand(s) required? |  |  |  | X |
| Simple Grasping (R or L) |  | X |  |  |
| Power Grasping (R or L) |  | X |  |  |
| Fine Manipulation (R or L) |  | X |  |  |
| Pushing/Pulling (R or L) |  | X |  |  |
| Reaching (above/below shoulder level) |  | X |  |  |
| Lifting/Carrying | Occasionally lift and carry objects (e.g., Laptop, Portable Projector, Briefcase, documents, etc.) weighing 10-15 lbs. | | | |

**SECTION J: SIGNATURE**

By signing this document, I acknowledge I understand all requirements and information stated above and understand the duties may be modified in accordance with the established job specifications for the class and in conjunction with office needs and have received a copy of this duty statement.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Signature Date

I have discussed and provided a copy of this duty statement to the employee named above.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor’s Signature Date