**OFFICE OF THE STATE CONTROLLER**

DUTY STATEMENT

|  |  |
| --- | --- |
| **EMPLOYEE NAME**  TBD | **DIVISION**  Information Systems |
| **CLASSIFICATION TITLE**  Information Technology Manager II | **UNIT NAME - LOCATION**  Information Security Office (ET) Sacramento |
| **WORKING TITLE**  Chief Information Security Officer | **POSITION NUMBER**  051-340-1406-xxx |
| **Information Technology Domain**  Information Security Engineering | **EFFECTIVE DATE**  TBD |

**SECTION A: GENERAL DESCRIPTION**

Under the broad administrative and policy direction from the Chief Information Officer (CIO) in the Information Systems Division (ISD), Chief Administrative Officer (CAO), and Chief Operating Officer (COO), the incumbent is tasked with the strategic leadership and administration of the State Controller’s Office (SCO) Enterprise Information Security Program. As the SCO’s Chief Information Security Officer (CISO), the incumbent’s responsibilities extend to the formulation, oversight, and administration of the SCO’s Enterprise Information Security Program’s standards, procedures, guidelines, safeguards, initiatives, and processes. The CISO ensures a systematic, disciplined approach to evaluating and improving the effectiveness of information security risk and internal control management, security assurance, statutory compliance, and governance at the SCO.

The incumbent will be responsible for developing and monitoring program goals, objectives, and budget. This level is responsible for the personnel development activities of personnel within the security office, contract negotiations, and business services. The incumbent will also be responsible for developing policy and strategic plans; establishing strategic goals and longer-range planning; and determining new enterprise-wide direction and policy decisions. 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% | Steers the enterprise-wide development and tactical execution of a sophisticated information security and privacy program to ensure the uncompromised confidentiality, integrity, availability, and privacy of assets under SCO’s dominion. Elevates and refines the organization's security policy, strategy, and advanced practices, working closely with C-suite executives to solidify security and privacy protocols. Aligns information security endeavors with SCO's constitutional authority and organizational objectives, acquiring endorsement from top-tier stakeholders. Orchestrates risk assessment and risk management initiatives, embedding them into each business unit's operations. Instates a rigorous, risk-based assessment framework for engaging with external partners, suppliers, and other third parties, and monitors contractual obligations to manage residual risks. Oversees incident response and containment strategies, ensuring a fortified defense against internal and external security threats while preserving SCO's reputation and regulatory standing. Keeps a vigilant eye on the evolving threat landscape and proactively advises key stakeholders on risk mitigation strategies. Leads talent acquisition, development, and retention strategies, ensuring a specialized skill set within the team to support both current and evolving organizational demands. Sets clear performance goals for the team and fosters a high-performance environment. Maintains rigorous compliance with organizational protocols and ensures staff adherence. Provides operational leadership, overseeing task assignments, quality assessment, and timelines, while promoting continuous skill development and training. Executes an advanced analytical and technical training agenda to ensure a forward-leaning skill set within the team. |
| 25% | Orchestrates the optimization of the information security and privacy governance architecture, incorporating an advanced hierarchical governance framework that includes specialized committees such as the Information Security Executive Council. Delivers comprehensive, high-level reports on the current state and emerging threats of the SCO's Advanced Enterprise Information Security Program to executive management and senior business leaders, as part of a sophisticated enterprise risk management strategy. Develops and oversees an executive-level information security awareness training initiative, targeted not only at employees and contractors but also at high-stakes external partners, and implements KPI-driven metrics for evaluating the program's effectiveness. Collaborates with interdisciplinary leadership committees to ensure a uniform, yet flexible, application of security, privacy, risk management, and compliance policies across all business units and technological infrastructures. |
| 20% | Steers and formulates advanced strategic frameworks for SCO’s information security and privacy initiatives, prioritizing a seamless integration between privacy, security, and Divisional business objectives. Amplifies the implementation of data analytics to bolster predictive security measures and enhance protective mechanisms across SCO. Insurers that all information under SCO’s ownership or control adheres rigorously to evolving global legal and regulatory frameworks, including but not limited to data privacy and sovereignty mandates. |
| 15% | Serves as a leading authority on advanced information security and privacy practices, shaping internal policy and industry standards. Engages executive IT and business stakeholders to strategically manage and mitigate information security risks, emphasizing shared accountability. Consistently integrates real-time government and industry intelligence to stay ahead of emerging threats and vulnerabilities. Orchestrates synergistic internal collaborations among the information security team, line-of-business leaders, compliance units, audit functions, physical security, legal, and HR management to foster organizational alignment on security protocols. Nurtures a network of external partnerships with industry thought leaders, ecosystem allies, vendors, and other pertinent entities to collectively address evolving cybersecurity trends, findings, and risks. Interfaces with external regulatory and advisory bodies, ensuring that SCO's security posture is in line with emerging threat vectors identified by these organizations. Aligns security protocols with Information Technology teams to ensure security-by-design across architecture, infrastructure, and application development initiatives. |

**SECTION C: NON-ESSENTIAL FUNCTIONS**

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

**SECTION D: ADA REQUIREMENT**

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 (e.g., methods for assessing and mitigating risk, such as Risk Management Framework (RMF) requirements.
* Knowledge of state and federal laws, regulations, policies, guidelines (NIST Special Publications) and ethics as they relate to information security and privacy.
* Knowledge of information security and privacy principles.
* Knowledge of physical and cyber threats and vulnerabilities.
* Knowledge of specific operational impacts of information security lapses.
* Knowledge of information technology (IT) architectural concepts and frameworks.
* Knowledge of resource management principles and techniques.
* Knowledge of system life cycle management principles, including software security and usability.
* Knowledge of the organization’s enterprise information technology (IT) goals and objectives.
* Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.
* Knowledge of the organization's core business/mission processes.
* Knowledge of compliance auditing.
* Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.
* Knowledge of cryptography and other security technologies.
* Knowledge of organizational process improvement concepts and process maturity models.
* 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.

**Skills:**

* 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.

**Abilities**

* 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 think critically.
* 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 to understand the basic concepts and issues related to information security and its organizational impact.
* 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.

**Desirable Qualifications**

In addition to evaluating each candidate's relative ability, as demonstrated by quality and breadth of experience, the following factors will provide the basis for competitively evaluating each candidate:

* Possession of a current CISSP, CISM and/or CCISO information security professional certification.
* Demonstrated knowledge and experience in security risk management, planning and assessment/auditing.
* Demonstrated experience managing the information and physical security controls associated with sensitive and confidential data and assets; and, vulnerability and configuration assessment of systems, applications, services and other infrastructure foundational components.
* Demonstrated experience developing, planning, and implementing enterprise information and physical security programs for business functions that include large financial and moderate level IT asset security risk.
* Demonstrated experience interacting with, influencing, and building business relationships with multiple stakeholders and departments, including high-level executives.
* Demonstrated ability and experience establishing enterprise information and physical security standards, procedures, guidelines and recommendations.
* Demonstrated experience and ability to communicate information regarding security or privacy standards, technology and issues effectively to business and IT management and other staff.
* Demonstrated ability to solve problems, promote new ideas, and develop new approaches to achieve the SCO’s vision.

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

The incumbent, as the Chief Information Security Officer (CISO), will provide strategic oversight and administration of the State Controller’s Office (SCO) Enterprise Information Security Program and make high-level consultative recommendations concerning the security and privacy of SCO’s environments. This includes, but is not limited to, all business programs, operations, projects, data, networks, systems, applications, personnel, and facility physical security.

The effect of this strategic oversight, administration, and consultative recommendations activities will have statewide and enterprise-wide impacts, affecting the efficiency and effective operation and performance of SCO environments and their overall security posture.

Errors in oversight, administration, or recommendation judgment and decision-making could result in lost funding, project failure, failed business strategy, poor customer service and performance, risk exposure, and loss of business continuity. This could also lead to missed business opportunities and budget implications.

Such errors could result in a degradation of 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 frequent contact with senior-level and high-level entities in unique situations where it can be challenging to establish the contact and identify goals. The incumbent consults with or advises management, administrative or executive staff on the planning, development, implementation, and coordination of IT issues.

Frequent contact with vendors is required to assess new technologies and contractors to provide oversight, negotiate contract modifications, and analyze compliance with contract specifications. Contacts occur in conferences, meetings, hearings, or presentations involving problems or issues of considerable consequence or importance.

Contacts typically have diverse goals or objectives requiring a common understanding of the problem and a satisfactory solution by convincing individuals, arriving at a compromise, or developing suitable alternatives. Contacts are to justify, defend, negotiate, or settle matters involving significant or controversial issues.

The incumbent also has contact with other state agencies, federal government, and local governments.

**SECTION H: WORK ENVIRONMENT**

The incumbent will work in a multi-story climate-controlled office under artificial lighting. Travel to customer locations, primarily in Sacramento County, will occur on a regular basis. When traveling, the incumbent may be subject to the elements of the destination. The incumbent is expected to adhere to a consistent work schedule averaging 40 hours per week. The incumbent may be required to work outside of normal business hours.

**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