**Department of Real Estate**

Position Duty Statement

RE 108 (rev. 07/20)

|  |
| --- |
| Employee’s Name |
| Classification TitleInformation Technology Manager I | Division/Section/UnitInformation Technology Division/Information Security Office |
| Working TitleChief Information Security Officer | Geographic LocationSacramento |
| Position Number414-140-1405-XXX | Effective Date  |

Under general direction of the Assistant Commissioner, Information Technology Services/Chief Information Officer (CIO) and working as the Chief Information Security Officer (CISO), the Information Technology Manager’s role is to provide vision and leadership for developing and supporting security initiatives such as development and implementation of the strategies, processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and non-digital information. The CISO supports the planning and implementation of enterprise IT systems, business operations, and facility defenses against security breaches and vulnerability issues. This individual is also responsible for auditing existing systems, while directing the administration of security policies, activities, and standards. This position is in the Information Security Engineering domain. Duties include, but are not limited to the following:

1. Specific Assignments [w/ Essential (E) / Marginal (M) Functions]

**40% Strategy and Planning**

Develop and implement a long-term information security strategy and framework to ensure the department’s information assets are adequately protected. Lead strategic security planning, working with leadership to achieve business goals by prioritizing defense initiatives and coordinating the evaluation, deployment and management of current and future security technologies. Develop and communicate security strategies and plans to department staff, partners, customers, and stakeholders. Participate in the design and implementation of disaster recovery and business continuity plans, procedures, audits, and enhancements. **(E)**

**25% Policy and Compliance Management**

Develop, implement, maintain, and oversee enforcement of policies, procedures, guidelines, and associated plans for system security administration and user system access based on departmental strategy, the State Administrative Manual, the State Office of Information Security policies and guidance and other applicable state and federal regulations. Coordinate their review, approval and dissemination. Review and update information security policies, standards, guidelines, processes, and procedures as needed to prevent new threats and vulnerabilities. Monitor and audit compliance with information security policies, standards, guidelines, processes, and procedures and provide status and enforcement recommendations to the CIO. **(E)**

**20% Risk Management**

Develop and maintain the department’s information security risk management program components including but not limited to risk assessment, mitigation, and evaluation.

Conduct and lead formal risk assessments on a regular basis for all major systems and information processing activities to ensure compliance with laws, statutes, regulations and security policies. Participate in Independent Security Assessments (ISAs). Develop responses to ISA findings, plan actions and milestones to address the findings, and coordinate the implementation of planned actions to address the findings. Implement, direct and manage the data capture and analysis activities to detect potential fraud and exposure; identify solutions and coordinate their implementation to prevent fraud and exposure. Develop and maintain asset management security controls throughout the lifecycle of all information assets. Create, implement, and maintain formal processes to mitigate information security vulnerabilities. Establish an incident response plan and coordinate responses to security incidents as necessary. Collaborate with IT management and the privacy officer to establish and maintain a system for meeting privacy policies. **(E)**

**10% Training and Communications**

Educate staff on information security and privacy protection responsibilities. Manage and ensure security training is provided to all staff at the appropriate frequency. Collect security awareness training metrics. Maintain awareness of the trends and benchmarks in the information security landscape and communicate the information to the appropriate staff. **(E)**

**5% Marginal Functions**

Perform other duties as related. **(M)**

1. Supervision Received

 The Information Technology Manager I reports directly to, and receives the majority of assignments from, the Chief Information Officer; however, direction and assignments may also come from the Chief Deputy Commissioner or Real Estate Commissioner.

1. Supervision Exercised

The Information Technology Manager I supervises the Information Security staff. This supervision includes, but is not limited to, management and planning, prioritizing tasks, scheduling, assigning, and overseeing work activities. The incumbent has signature authority to approve staff schedules, leave requests, timesheets and merit salary adjustments. The incumbent performs performance appraisals and assists staff with training and improvement plans.

1. Administrative Responsibility

The Information Technology Manager I is responsible for managing and coordinating the activities of the Information Security Office for the Department of Real Estate.

1. Personal Contacts

The Information Technology Manager I has contact with all levels of the DRE staff, consultants, vendors, California Department of Technology staff, control Agency staff, and other government agencies. Contacts may be initiated with other departments, governmental agencies, and private companies concerning information system technologies as they relate to the performance of this position.

1. Actions and Consequences

The Information Technology Manager I will make decisions that impact the functionality of DRE technology applications and solutions. Failure to properly administer duties using good judgment, logic, and discretion, may result in an information security breach, poor performance or unusable systems and applications, and prevent the DRE end users from effectively performing their duties. Also, substantial workload backlogs may occur, online consumer services may be unavailable, and the DRE may be unable to carry out mandates designed to protect consumers, licensees, and applicants.

1. Functional Requirements

The Information Technology Manager I is a Work Week Group E employee, is expected to work an average of 40 hours per week each year and may be required to work specified hours based on the business needs of the office. The incumbent must occasionally move about inside the office to access office machinery. The incumbent must constantly operate a computer and other office productivity machinery, such as a copy machine. The incumbent must be able to remain in a stationary position 50% of the time.

1. Other Information

The Information Technology Manager I must be able to reason logically and creatively and utilize a wide variety of skills to resolve enterprise-wide technical issues, application development, and multiple system interface issues. Additionally, this position must have the ability to communicate and resolve business-related issues/problems that require a technology solution. Incumbent must be able to develop and evaluate alternatives, research and present ideas and information effectively both orally and in writing. Incumbent must be able to consult with and advise interested parties on IT subjects; gain and maintain the confidence and cooperation of those contacted; accurately assign priorities to multiple projects at any given time and to remain flexible. The incumbent shall operate to protect the cybersecurity of individual departmental staff and all data c. The incumbent's policy direction must be adaptable to the rapidly changing technology landscape.

This position is subject to the provisions of 2 Cal. Code of Regs. §18730, which contains the Conflict of Interest Code for the Department of Real Estate.

**I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation.** (If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the Health & Safety analyst.)

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

Employee Signature Date

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

Employee’s Printed Name – Classification

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

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

Supervisor Signature Date

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

Supervisor’s Printed Name – Classification

**New: 04/2022**