

**Duty Statement**

Information Technology Services Division

Duty Statement

**Classification:** Information Technology Manager I

**Working Title:** Information Security and Privacy Officer

**Domain:** Information Security

**Name:** Vacant

**Scheme/Class Code:** 1405

**Position Number:** 813-064-1405-001

**FLSA Status:** FLSA Exempt

**Division:** Information Technology Services Division (ITSD)

**Branch:** Information Security Office

**Section/Unit:** Information Security Office

**Primary Assignment:** Oversee and manage the Department's Information Security and Privacy Programs

**Job Objectives:** Under the general direction of the Deputy Director over the Information Technology Services Division (ITSD), Chief Information Officer (CIO), the Information Security and Privacy Officer (ISPO) establishes and manages the Department of Rehabilitation (DOR) information security and privacy program frameworks and risk and vulnerability management program, policies, and training to ensure the continued security and integrity of enterprise systems and data. The ISPO coordinates all information system audits with state and federal control agencies and is responsible for collecting and maintaining system security data required by state and federal control agencies. The ISPO advises the Directorate of security and privacy incidents and risks that threaten the confidentiality, integrity, and availability of the DOR's information assets.

This position formulates and administers departmental security, privacy, and risk management programs and policies. The incumbent must have strong leadership and organizational skills, knowledge of state and federal security and privacy requirements, experience performing risk analysis and risk management, demonstrated ability to identify and respond to threats, and ability to lead and respond to security and privacy incidents. The incumbent must possess strong customer service skills and knowledge of state and departmental administrative processes.

1. Essential Functions

**35%** **Information Security Office Oversight, Management, and Planning**

Plans, organizes and directs the activities of the Information Security Office responsible for development, implementation, and maintenance of all necessary information security and privacy policies, standards, guidelines, and training required for comprehensive Information Security, Privacy, and Risk and Vulnerability Management Programs. Ensures a clear and consistent approach in the planning, implementation and maintenance of security technology and tools that protect DOR information assets and works to institutionalize risk management throughout the department. Manages Information Security and Privacy Office (ISPO) staff, assigns work, monitors, provides guidance, and evaluates performance.

Leads ISPO staff in implementing industry best practices, identifying and responding to threats, performing vulnerability assessments, investigating security and privacy incidents, and complying with state and federal security policies. Manages the design, development, implementation and operation of the information security and privacy program and policies, by using knowledge of applicable statutes and guidelines, including California Civil Code, SAM, SIMM, National Institute of Standards and Technology (NIST), and directives published by Social Security Administration. Oversees planning of the department's security architecture and technical recovery activities, including maintaining and updating the department's Technical Recovery Plan.

As a member of the ITSD’s and the Department’s senior leadership team, collaborates with the CIO, ITSD Branch Chiefs, and senior leaders throughout the organization engage in IT systems planning related to information security and privacy, organizational issues, and strategic planning. Collaborates with California Health and Human Services Agency (CHHS) ISOs and the California Office of Information Security (COIS) to ensure alignment with statewide security and privacy initiatives and participate in security planning activities.

Provides advice and assistance to executive leadership (DOR Directorate, Deputy Directors, and senior leadership) on specific information security and privacy assessment and audit issues including response activities that may result in press releases, substantial costs, and potential lawsuits and fines.

Provides leadership and a forum for ITSD managers and staff to discuss information technology security and privacy architectures, standards, organization and allocation of resources. Identifies, reviews, and recommends appropriate action to be taken in response to sensitive information security and privacy issues. Reviews and approves security plans and procedures, technical recovery plans, project security requirements, formal submissions to state and federal entities, and exceptions to policy.

**30%** **Risk and Vulnerability Management:**

Leads implementation and maintenance of risk and vulnerability management practices. Leads senior leadership, program, legal, and technology staff in identifying potential business risks, regulatory noncompliance and legal liabilities regarding systems, applications, and business processes. Coordinates discussions with key stakeholders to enable better risk-based decision-making. Provides a balanced view of the DOR’s information security risk relative to organizational culture and program impacts. Delivers a comprehensive view of the information security risks to assist the Directorate in identifying risk concerns to the department.

Leads the department in identifying vulnerabilities in applications and systems that pose risks to the department. Implements vulnerability scanning solutions and identifies and tracks vulnerabilities through remediation. Coordinates regular analyses and assessments to identify potential risks to the security, confidentiality, integrity, and availability of the department's information assets. Determines the probable loss and consequences of identified threats and assesses the likelihood of such occurrences. Identifies and recommends cost-effective measures to mitigate security threats and reduce risk to an acceptable level.

Prepares regular reports for the DOR's Directorate and executive staff to document risk assessments, propose security management measures, identify resources necessary for security and privacy management, and quantify and explain the amount of remaining risk to be accepted by the DOR. Provides required reports and makes recommendations to control agencies on implementation of the DOR's security and privacy functions and ongoing compliance with the state's risk management policies.

**20%** **Privacy Program**

Manages the privacy programand collaborates with the DOR privacy attorney to ensure all data is appropriately classified. Plans and develops privacy strategies consistent with the DOR's business goals and objectives and the business needs of the department. Formulates and implements strategies to address information security and privacy needs and to determine the need and appropriateness of proposed security and privacy provisions. As needed, develops, implements, and maintains a data classification process for the DOR's data in accordance with state and federal rules and regulations. Leads implementation of data protection technology solutions to protect the collection or creation, storage, use, transmission and disposal of data. Educates department staff on the information classification process and monitors and tracks classification activities.

Ensures that Privacy Threshold Assessments/Privacy Impact Assessments are completed for all proposed and existing systems. Determines the risks and effects of collecting, maintaining, and disseminating information in identifiable forms in electronic information systems. Examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.

Develops and implements policies and procedures for reporting and monitoring incidents involving intentional, unintentional, or unauthorized disclosure, use, modification, access, or destruction of the DOR's information assets. Leads investigations of security incidents, including responding to, investigating, tracking, resolving, and reporting to management, law enforcement, and state control agencies. Oversees investigations of alleged incidents of security violations. Coordinates with DOR privacy staff to address privacy issues including, but not limited to, developing and distributing security and privacy breach notifications. Leads post-incident reviews and development of action plans with staff to implement measures that reduce risk of similar incidents.

**10%** **Represents the DOR** at security conferences, forums, and meetings with security organizations, state data centers, and control agencies to identify information security practices, trends, requirements, rules, and regulations applicable to the DOR. Educates executive staff, senior leadership staff, and division management regarding state and federal security and privacy requirements and industry best practices for the proper classification, use, and protection of the DOR's information assets. Responds to written and verbal inquiries from department management and external parties on security issues.

1. Marginal Functions

**5% Continuing Education and Collaboration**

Continuously develops and enhances information security knowledge by ensuring thorough familiarity with the available tools, methods and procedures to complete assignments; researches, investigates, and keeps abreast of trends in information security; and attends training, conferences, and webinars. Participates in and facilitates division and team meetings and other team activities.

1. Supervision Received

The Information Technology Manager I receives supervision from the ITSD Deputy Director, CIO.

1. Supervision Exercised

The Information Technology Manager I exercises supervision over two Information Technology Specialists II and three Information Technology Specialists I.

1. Administrative Responsibility

Adheres to departmental, divisional and unit policies and procedures.

1. Personal Contacts

This position acts as the DOR liaison with outside parties in matter of information security including audits. The Information Technology Manager I interacts with staff at all levels of the department, representatives of other departments and control agencies such as Health and Human Services Agency, California Office of Information Security, Department of Justice's Privacy and Enforcement Protection Unit, Department of Finance, Department of General Services, Office of Systems Integration and California Department of Technology. The position works closely with and consults with the DOR Deputy Directors and senior management on information security and privacy incidents, activities, policies, and procedures.

1. **All Times**

Communicate effectively in a professional, tactful, respectful manner with individuals from varied experiences, perspectives and backgrounds, by telephone, email and other technologies as well as in-person; provide excellent customer service to both internal and external customers; ensure the timely completion of assignments; attempt to resolve individual concern at the lowest possible level; offer other dispute resolution options, and elevate to next level if needed; use initiative, problem solving skills, organizational skills, good judgment, and resourcefulness.

1. **PERFORMANCE REQUIREMENTS:**

The ISPO is expected to demonstrate an extensive knowledge of data processing concepts and current trends to establish and maintain a comprehensive information security program. The program covers such critical areas as planning and administration of security, privacy, and risk management programs, access control, network security measures, Internet and e-mail issues, setting security and privacy policies, standards, and procedures, security architecture, gaining management and organization support, legal aspects of information security, and the future of information security in the organization. The incumbent is expected to maintain an in-depth knowledge of industry best practices in security, privacy, and risk management and requirements imposed by federal and state agencies. Further, the ISPO must exercise a high level of discretion in dealing with confidential security measures and issues.

Note: It is the policy of the Department of Rehabilitation to provide equal employment opportunity to all employees and applicants; that employees have the right to work in an environment free from discrimination; that consumers have the right to receive services free from discrimination in compliance with local, state, and federal laws.

I have read, understand, and agree to perform the above listed duties and all duties typically performed by this classification. I certify that I possess the essential personal qualifications and will perform these duties with integrity, initiative, dependability, good judgment, and will work cooperatively with others when performing the assigned duties as described above.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Employee’s Signature |  | Date |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Supervisor’s Signature and Title |  | Date |