STATE OF CALIFORNIA
CIVIL RIGHTS DEPARTMENT
DUTY STATEMENT

Employee Name	Classification Name	Position Number
Vacant	Information Technology Specialist II	326-500-1414-00X
Division/Unit	**Date**	**Prior Pos. # (if applicable)**
Information Technology	3/9/23	326-500-1405-002

SUMMARY OF RESPONSIBILITIES

Under general direction of the Information Technology Manager I (ITM I) and with coordination with the Chief Information Officer(CIO), the Information Technology Specialist II (ITS II) functions as the Chief Information Security Officer (CISO) for the Civil Rights Department (CRD). The incumbent is responsible for establishing and maintaining all departmental information security policies and plans and ensuring that they align with all Federal and State security regulations. Serves as a member of the CRD Infrastructure and Operations team to ensure that security policy is appropriately implemented in all Information Technology systems and assets.

Essential Functions:

25% Using industry best practices, the CISO updates and creates CRD departmental Security policies and plans in accordance with applicable State, Federal, and Industry Information Security guidelines and Standards. Tasks include creating, updating, approving, and publishing all CRD Information Security Policies and Plans to ensure that they are always compliant with current State, Federal and industry requirements.

25% The CISO monitors Information Security trends, including applicable state and Federal policies to ensure that CRD remains compliant with all new Information Security practices as they become implemented. The CISO represents CRD at all agency and statewide security forums in order to collaborate with peers and gain knowledge of statewide and agency level security requirements. Represents the department on any security audit activities and provides regular updates on action items and findings resulting from said audits.

15% Conducts product research and analysis; and recommends changes or updates to the infrastructure. Attends training regularly to ensure knowledge of current information security practices and techniques. Solves a range of complex policy and technical problems; assists with hardware and/or software installation and testing, user training, network connectivity troubleshooting, and device monitoring applying to Information Security.

10% The CISO provides regular guidance and training to all CRD staff to ensure that all employees follow appropriate information security practices, and that the department is compliant with state and federal security training requirements. Additionally, the CISO develops and publishes formal annual security awareness training for all CRD staff.

10% Assists the CRD Security Architect with Information Security Monitoring duties including, but not limited to Nessus vulnerability scans, Endpoint protection logs, Intrusion Detection and Prevention logs, and other security related systems.

10% Works closely with the CRD Operations Support staff to ensure all CRD devices meet or exceed State of California standards for data security and protection. This includes ensuring all cloud and on-premises infrastructure is configured, patched, and upgraded based on approved and documented California and CRD information security policies and practices.

Marginal Functions:

5% Assists in providing training to technical staff and other users on all departmental information securitytechnology applications. Provides input in the preparation of user guides and technical documentation on departmental applications. Performs other duties as required.

Desirable Qualifications:

- Experience in leading and managing concurrent complex infrastructure projects.
- Experience in communicating effectively verbally and in writing.
- Experience in managing and negotiating multiple and/or changing priorities in a heavy workload situation.
- Demonstrated experience in leadership, diplomacy and courtesy.
- Experience in establishing and maintaining the confidence and cooperation of others contacted during the course of work.
- Experience analyzing data, drawing sound conclusions and presenting ideas and information effectively both orally and in writing.
- Experience in the maintenance and management of information security solutions.
- Experience creating information security policies and procedures.
- Experience in the management of Microsoft Server environments, including Active Directory, Azure, SCCM, Intune and Office/Microsoft 365.
- Knowledgeable in Scripting Languages such as PowerShell or Python.
- Experience in managing and configuring security solutions such as Nessus Professional software and PEN testing applications.
- Experience with SIEM solutions such as Splunk ES, Microsoft Sentinel, etc.
- Experience in managing and supporting Endpoint Protection platforms, such as Defender.

Work Environment, Physical or Mental Abilities:

The demands described here are representative of those that must be met by the incumbent to successfully perform the essential functions of the job with or without a reasonable accommodation.

- Requires ability to effectively handle stress, and work in a noisy and fast paced environment
- Requires daily use of a personal computer and related software applications at a workstation
- Requires ability to complete tasks that require repetitive hand movements in the performance of daily duties
- Requires prolonged sitting and/or standing in a workstation for 6.5 to 7 hours per day
- Requires dependability and excellent attendance record
- Willingness to work irregular hours

Supervision Received:

The ITS II receives general supervision from the Information Technology Manager I (ITM I).

Supervision Exercised:

None.

Personal Contacts:

The ITS II may have daily contact with departmental management and staff, and regularly has contact with control agency representatives, data center representatives, other state agencies, and private industry.

Job Requirements:

Activities required to perform the essential functions of this position include the ability to communicate effectively, produce written correspondence, and comprehend written instructions, correspondence and manuals, and reason logically. The ITS II position requires excellent writing and analytical skills; the ability to work independentlyand to speak and write clearly, concisely, and accurately; to reason logically and creatively in resolving problems; skill in dealing effectively with others; willingness and ability to accept responsibility and meet deadlines; and ability to manage multiple projects with different time frames.Adhere to the laws, rules, policies and procedures as outlined in the Department's Directives, State Administrative Manual, Statewide Information Management Manual, California Multiple Awards Schedules, Supervisor's Manual, Clerical Manual, Case Analysis Manual, and any directions givenby all appropriate managers.

Actions and Consequences:

The ITS II is in a sensitive position involving critical departmental data assets, and the security of said assets. Failure to use good judgment in design and implementation or to ensure the timely processing of requests could result in data asset compromise. Failure to use good judgment in handling sensitive and confidential information could result in sensitive information being released to unauthorized persons and/or incorrect information used to make management decisions.

Employee Certification:

I have read and understand the duties as described above for the Information Technology Specialist II. I meet the job requirements as described above and can perform the essential functions with or without a reasonable accommodation.

_______________________________ _______________________

Employee’s Signature Date

_______________________________ _______________________

Supervisor’s Signature Date