Classification: Information Technology Specialist I
Position Number: 880-280-1402-063

DUTY STATEMENT

☐ **CURRENT** ☒ **PROPOSED**

RPA Number: 26-280-008	**Classification Title:** Information Technology Specialist I	**Position Number:** 880-280-1402-063
Incumbent Name: VACANT	**Working Title:** Security Analyst	**Effective Date:** **TBD**
Tenure: Permanent	**Time Base:** Full time	**CBID:** R01
Division/Office: Division of Information Technology	**Section/Unit:** Information Security Office	
Supervisor's Name: Angela Ramirez	**Supervisor's Classification:** Information Technology Manager I	

Human Resources Use Only:	
HR Analyst Approval: Rebecca Ramirez	**Date:**

General Statement

Under the direct supervision of an Information Technology Manager I (ITM I) and consistent with good customer service practices and the goals of the State and Regional Board's Strategic Plan, the incumbent is expected to be courteous and provide timely responses to internal/external customers, follow through on commitments, and to solicit and consider internal/external customer input when completing work assignments.

Position Description

The Information Technology Specialist I (ITS I) will help with the implementation of security controls, tools, plans, policies, risk assessments, and incident response for the California State Water Resources Control Board (SWRCB). The ITS I will also assist in ensuring the organization's compliance and observance of state and federal security regulations, standards, and best practices to secure information assets, remediate vulnerabilities, and promote a secure computing environment that provides consistent confidentiality, integrity, and availability of SWRCB systems and information.

The incumbent will primarily perform tasks in the Information Security Engineering and Information Technology Client Services domains.

Essential Functions (Including percentage of time):	
35%	Assist with configuring, updating, troubleshooting, and supporting security tools managed by the Information Security Office, such as the System Information Event Management (SIEM) system, vulnerability scanners, penetration testing platform, web application firewalls, and other security appliances and their components. Perform regular security system maintenance while adhering to established change management processes. Respond to correspondence and service requests assigned to the Information Security Office professionally and thoroughly.
30%	Perform continuous event monitoring, including validating alerts, distinguishing between benign and possible malicious attacks and intrusions, and taking appropriate remediation steps using an endpoint detection and response (EDR) solution. Proactively monitor security-related tools and services for signs of potential malicious activity and take appropriate remediation steps. Participate in security incident response, investigations, and forensics, such as assisting in determining the scope, urgency, and impact of security incidents; reconstructing event timelines; conducting root cause analysis; and handling artifacts. Respond to security-related threats as part of the Information Security Office. Conduct computer forensic investigations. Maintain contact with other State agencies and security units such as the California Cybersecurity Integration Center (Cal-CSIC).
25%	Assist with reviewing and evaluating non-standard software requests, including, but not limited to, researching the functionality, security configuration, terms of service agreements, and other factors, before presenting information for a final decision. Create security training campaigns and assist in developing and executing phishing exercises. Perform periodic reviews of security courses for accuracy and currency. Draft communications for department-wide dissemination covering topics such as annual training, security-related notifications, and other information security-related content. Utilize frameworks and manuals for compliance, such as National Institute of Standards and Technology (NIST) 800-53, the State Administrative Manual (SAM) 5300, and the State Information Management Manual (SIMM).

Marginal Functions (Including percentage of time):	
5%	Attend regularly scheduled Division of Information (DIT) staff meetings and training sessions. Participate in development activities to meet the needs of the organization and the individual. Maintain ongoing knowledge of threats and vulnerabilities and current cybersecurity trends, State and Federal legislation, regulations, and policies related to information security, and foundational information security methodologies and best practices.
5%	Perform other duties as required.

Typical Physical Conditions/Demands:

The job requires extensive use of a personal computer and the ability to sit/stand at desk, utilize a phone and a keyboard for extended periods of time. Ability to lift 15 pounds to retrieve files and/or documents.

Typical Working Conditions:

The incumbent works in a high-rise office building. The work schedule is Monday through Friday. Telework and hybrid workspace options may be available based on operational needs. Travel may be required.

Supervisor Statement

I certify this duty statement represents an accurate description of the essential functions of this position. I have discussed the duties of this position with the employee and provided the employee with a copy of this duty statement.

Supervisor Name	Supervisor Signature	Date
Employee Name	Employee Signature	Date