Classification: Information Technology Spec II
Position Number: 880-280-1414-025

DUTY STATEMENT

☐ **CURRENT** ☒ **PROPOSED**

RPA Number: 25-280-038	**Classification Title:** Information Technology Specialist II	**Position Number:** 880-280-1414-025
Incumbent Name: VACANT	**Working Title:** Information 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:	**Date:**

General Statement

Under the general direction of the Information Technology Manager I (ITM I) of the Information Security Office (ISO) and consistent with good customer service practice and the goals of the State and Regional Board's Strategic Plan, the incumbent is required to be courteous, communicate effectively and professionally (verbally and in writing) with team members and customers, follow through on commitments, provide timely responses and consider internal and external customer input when completing work assignments.

Position Description

The Information Technology Specialist II is a technical subject matter expert and security authority for security controls and tools, security plans, security policies and procedures, risk assessments, and incident response for the California State Water Resource Control Boards (SWRCB). The incumbent is involved in ensuring the organization's compliance and observance of state and federal privacy and 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 the SWRCB systems and information. The incumbent may perform tasks in the Information Security Compliance, Information Technology Project Management, Software Engineering, and System Engineering domains.

Essential Functions (Including percentage of time):	
30%	Develop and maintain information security-related policies, procedures, analyses, assessments, forms, and other required information security documentation. Collaborate closely with technical and program area subject matter experts. Ensure documents are current, clearly written, and align with SWRCB and State of California requirements. Prepare and submit reports and supporting materials and participate in activities in accordance with applicable state requirements, including the State Administrative Manual (SAM) and the Statewide Information Management Manual (SIMM), and other California Department of Technology directives. Apply frameworks and standards such as the National Institute of Technology (NIST) 800 series, SAM 5300, and SIMM to maintain compliant information security practices. Participate in and support information security audits and assessments. Research, monitor, and analyze cybersecurity and technology-related regulations and legislation at the federal and state levels and maintain knowledge of applicable federal and state laws, codes, and defined standards in addition to relevant SAM and SIMM policies relating to security.
30%	Review and assist with categorization of information systems and classification of data processed, stored, and transmitted by those systems. Assist in the development and maintenance of system security plans and business impact analysis. Develop and maintain information security plans, including but not limited to cyber risk, information security program, vulnerability management, incident response, etc. Review and document non-standard software requests and requested deviations from information security policy; evaluate risk and recommend mitigation measures to protect information asset confidentiality, integrity, and availability. Consult and interact with technical and program staff to provide security guidance, validate technical solutions, and ensure alignment with information security policies, SAM, SIMM, and industry best practices.
Marginal Functions (Including percentage of time):	
10%	Conduct research and perform security analysis on proposed system upgrades, new solutions, and process improvements; evaluate potential security impacts and provide risk-based recommendations that support SWRCB's security and information technology objectives. Plan and conduct Information Security and Privacy training activities, including creating security awareness training, conducting phishing exercises, generating reports, and composing all-staff notifications. Participate in various internal and external workgroups, committees, and various meetings and discussions requiring an Information Security perspective or consultation.
10%	Coordinate with technical teams to plan and implement security controls and measures to identify and mitigate security threats and vulnerabilities. Facilitate meetings with project teams and stakeholders and share knowledge through training materials and technical reviews.

10%	Respond to security-related threats as part of a Cybersecurity Incident Response Team (CSIRT). Conduct security incident management and investigations. Maintain contact with other State agencies and security units such as California Cybersecurity Integration Center (Cal-CSIC). Coordinate remediation efforts across IT teams, create a timeline of events, hold lesson-learned meetings, and generate post-incident reports. Update incident response procedures for incidents.
5%	Attend Division of Information Technology staff meetings and training sessions. Participate in professional development activities according to the needs of the organization and the individual. Participate in change management approval processes.
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 type on a keyboard for extended periods of time. Ability to lift 15 pounds, bend and reach above shoulders 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. 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 a copy of this duty statement.

Supervisor Name	Supervisor Signature	Date

Employee Name	Employee Signature	Date