☒Current ☐Proposed

STATE OF CALIFORNIA
California Victim Compensation Board
Rev. 07/22

# DUTY STATEMENT

| EMPLOYEE | | RPA # / JOB CONTROL # | |
|---|---|---|---|
| VACANT | | 25-029 / 457202 | |
| POSITION NUMBER | CLASSIFICATION | WORKING TITLE | |
| 040-410-1414-010 | IT Specialist II | IT Technical Security Engineer | |
| DIVISION | SECTION/UNIT | CBID | WWG |
| Information Technology | Information Security Section | R01 | E |
| WORKDAYS | WORK HOURS | TENURE | TIME BASE |
| Monday - Friday | Supervisor Discretion | Permanent | Full |

## CONFLICT OF INTEREST CLASSIFICATION

This position is designated under the Conflict-of-Interest Code and is responsible for making, or participating in the making of governmental decisions that may potentially have a material effect on personal financial interests. The appointee is required to complete a Form 700 within 30 days of appointment. Failure to comply with the Conflict-of-Interest Code requirements may void the appointment.

Conflict of Interest Classification? ☒ Yes ☐ No

## DEPARTMENT OVERVIEW

The California Victim Compensation Board (CalVCB) is a state program dedicated to providing financial assistance to victims of crime and helping them restore their lives. At CalVCB, we work to reduce the impact of crime on victims' lives. We reimburse crime-related expenses, connect victims with services and support, and do all we can to inform and empower victims.

**Our Mission:** CalVCB is a trusted partner in providing restorative financial assistance to victims of crime.

**Our Vision:** CalVCB helps victims of crime restore their lives.

## EMPLOYEE ACKNOWLEDGEMENT

I have read and understand the duties of this position and I certify that I possess essential personal qualifications including integrity, initiative, dependability, good judgment, and ability to work cooperatively with others; and a state of health consistent with the ability to perform the assigned duties as described above 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 Office of Civil Rights).

| EMPLOYEE'S NAME (Print) | EMPLOYEE'S SIGNATURE | DATE |
|---|---|---|
| | | |

## SUPERVISOR ACKNOWLEDGEMENT

I certify this duty statement represents current and 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'S NAME (Print) | SUPERVISOR'S SIGNATURE | DATE |
|---|---|---|
| | | |

# DUTY STATEMENT

(REV. 07/22)

**RPA 25-029**

## GENERAL STATEMENT

Under the general direction of the Information Technology Manager I, the Information Technology Specialist II, serves as the Information Technology (IT) Technical Security Engineer. Incumbents demonstrate a depth of leadership and expertise in Information Security Engineering and System Engineering domains. The position supports protection of mission critical systems and data by developing Information Security and Privacy (ISP) policies, processes, standards, and guidelines; assists in managing information security risks, CalVCB's Risk Register Plan of Actions and Milestones (RR-POAM) and provides support on information security program governance, vulnerability management, log management, security continuous monitoring, and software supply chain management. This position will primarily be responsible for work related to Information Security Office (ISO) activities and ongoing ISO related tasks.

CalVCB encourages a hybrid workplace model that is designed to support a distributed workforce of both remote and office-centered telework.

| % OF TIME PERFORMING DUTIES | DUTIES |
|---|---|
| 30% | **ESSENTIAL JOB FUNCTIONS:**<br><br>**IT Security Architecture, Risk and Security Assessment Support:**<br><br>• Design the information technology architectures and solutions to support security requirements in the areas of vulnerability management, log management, security continuous monitoring, and software supply chain management.<br>• Develop and ensure security solutions and technical artifacts are in place throughout all information technology systems and platforms.<br>• Lead and manage work on the Independent Security Assessments (ISA) and Information Security Program Audits (ISPA) by analyzing ISA/ISPA reports and work with CalVCB's ITD to provide recommendations on remediation and timelines, followed by documenting these in the Risk Register Plan of Actions and Milestones (RR-POAM).<br>• Conduct ongoing risk assessments to identify critical assets, threats, vulnerabilities, and exposures. Analyze and determine the likelihood and impact of information security risks. Maintain and log CalVCB internal risks identified and follow up with the risk owner for risk remediation, including documenting timelines for remediation.<br>• Summarize and present risk management and remediation progress to executive team and IT management team. Prepare confidential reports. Coordinate remediation activities with other groups (e.g., Infrastructure team, Service Desk, etc.).<br>• Monitor and assess security controls, conduct security impact analyses, and report system security statuses; perform risk assessments and recommend information technology solutions.<br>• Provide high level advice and assistance to ISO and executive management on specific information security related activities and audit issues. |

| | |
|---|---|
| 30% | **Vulnerability, Continuous Monitoring, Log and Software Supply Chain Management**<br><br>• Lead IT Security projects, develop and update and execute project plans, lead and mentor project teams.<br>• Lead in identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.<br>• Lead vulnerability management activities which include prioritizing risks and vulnerabilities, manage security patches, remediate, avoid, transfer and/or accept the risks.<br>• Lead efforts in Continuous monitoring of departments IT systems and networks, to detect security threats, performance issues, or non-compliance problems in an automated manner. Review weekly or monthly security reports to identify and report any non-compliance problems to management and follow up with respective team in remediation activities.<br>• Serve as an expert in Security log management comprising of log generation, transmission, storage, analysis, and disposal of security log data, ensuring its confidentiality, integrity, and availability.<br>• Serve as an expert in software supply chain security in securing the components, and activities in creation and deployment of software. |
| 25% | **Security Policies, Processes, Procedures, Standards, and Guidelines Activities**<br><br>• Serve as an expert on information security activities, governance, and compliance. Review and interpret current and new California state policies relevant to information security to understand and determine their impact on CalVCB's business needs and processes.<br>• Lead in effort to develop and maintain security policies to align with applicable laws, regulations, statewide policies, and CalVCB's strategic framework; assess existing policies and identify opportunities to improve alignment.<br>• Work with ISO to develop information security policies as necessary to support new laws and best practices and to comply with the California Department of Technology (CDT) Office of Information Security (OIS) Information Security program audits.<br>• Ensure security processes, procedures, standards, and guidelines align with applicable laws, regulations, statewide policies, and CalVCB's information security policies. Coordinate efforts to ensure procedures, standards, and guidelines are disseminated to personnel. |
| 10% | **Information Security Awareness Training and administrative tasks**<br>.<br>• Lead and manage Information Security Knowbe4 training system. Enroll new users, remove offboarding users, and generate weekly and ad hoc status reports for both executives and the CalVCB training team.<br>• Lead and manage quarterly phishing simulations tasks. Creation, maintenance, and execution of phishing simulation exercises. Provide status reports for executives upon conclusion of each exercise.<br>• Participates in formal and informal training programs to strengthen analytical skills and enhance knowledge of software tools and packages which would prove beneficial to end-users.<br>• Provides training to customers and business partners when required. |

| | |
|---|---|
| | **MARGINAL JOB FUNCTIONS:** |
| 5% | **Other Responsibilities**<br>Other duties may include but are not limited to presenting complex security topics in plain language to executives, management, and staff; attending agency and statewide information security related meetings, provide training and mentorship to staff. |

## DESIRABLE QUALIFICATIONS

- A Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM).
- Extensive knowledge of NIST and FIPS security standards and practices and their practical application.
- Experience with information security and privacy program management.
- Experience with information security and privacy risk assessment.
- Experience with security engineering.
- Experience with backup, recovery, and disaster preparedness.
- Proficient at delivering executive presentations, advanced written and oral communications skills.
- Proficient qualitative and quantitative analytical skills.
- Knowledge of information security and privacy program management concepts and frameworks.
- Knowledge of risk and vulnerability management concepts, terms, and methodologies.
- Knowledge of industry best practices and standards for IT systems, services, and processes
- Knowledge of security industry standards, concepts, practices, methods, and principles.
- Knowledge of the role and responsibility of various sections within an IT organization.
- Knowledge of the role and responsibility of various State control agencies.

## PERSONAL CHARACTERISTICS and EXPECTATIONS

- Demonstrated ability to act independently and as a member of a team with open-mindedness, flexibility, and tact.
- Ability to effectively handle stress and deadlines in a fast-paced work environment.
- Ability to problem-solve and use critical and creative thinking to effectively perform work.
- Display good interaction skills and the ability to deal professionally, congenially and in a personable manner with the public, other governmental entities, and staff at all levels.
- Communicate successfully in a diverse community as well as with individuals from varied backgrounds.
- Understand, follow and enforce all safety rules and procedures.
- Be supportive of management and coworkers.
- Maintain the confidence and cooperation of others.
- Ensure deadlines are met.
- Manage multiple & changing priorities.
- Maintain acceptable, consistent, and regular attendance.
- Develop and maintain knowledge and skill related to the job.
- Complete assignments in a timely and efficient manner.

## PHYSICAL ABILITIES

- Typical work requires prolonged sitting using a computer and telephone.
- Common eye, hand, and finger dexterity is required for most essential functions.
- Grasping and making repetitive hand movements in the performance of daily duties.
- Some carrying/moving of objects up to thirty pounds.