☒Current ☐Proposed

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

DUTY STATEMENT

EMPLOYEE		RPA # / JOB CONTROL #	
Vacant		25-041 / 463828	
POSITION NUMBER 040-410-1414-011	CLASSIFICATION IT Specialist II	WORKING TITLE IT Technical Security Engineer	
DIVISION Information Technology	SECTION/UNIT Information Security Section	CBID R01	WWG E
WORKDAYS Monday - Friday	WORK HOURS Supervisor Discretion	TENURE Permanent	TIME BASE Full-time

CONFLICT OF INTEREST CLASSIFICATION

This position is designated under the Conflict-of-Interest Code and is responsible for making, or participating in the making, 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 a 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 with a copy of this duty statement.

SUPERVISOR'S NAME (Print)	SUPERVISOR'S SIGNATURE	DATE

DUTY STATEMENT

(REV. 07/22)

RPA 25-041

GENERAL STATEMENT

Under the general direction of 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; manages information security risks, CalVCB's Risk Register Plan of Actions and Milestones (RR-POAM) and provides support on information security & privacy program governance, incident management, cloud security monitoring, continuous monitoring, threat intelligence platform, data loss prevention, and insider threat detection 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:** **IT Security Architecture, Risk and Security Assessment Support:** • Design the information technology architectures and solutions to support security requirements in the areas of cloud security monitoring, continuous monitoring, threat intelligence platform, data loss prevention, and insider threat detection. • Develop and ensure security solutions and technical artifacts are in place throughout all information technology systems and platforms. • Lead and manage work on the Independent Security Assessment (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). • Conduct ongoing risk assessments to identify critical assets, threats, vulnerabilities, and exposures. Analyze and determine the likelihood and impact of information security and privacy risks. Maintain and log CalVCB internal risks identified and follow up with the risk owner for risk remediation, including documenting timelines for remediation. • 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.). • Monitor and assess security controls, conduct security impact analyses, and report system security statuses; perform risk assessments and recommend information technology solutions. • Provide high level advice and assistance to ISO and executive management on specific information security related activities and audit issues.

30%	**Continuous Security and Cloud Security Monitoring, Data Loss Prevention, Threat Intelligence, Insider Threat Management** • 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 teams in remediation activities. • Develop processes that allow organizations to review, manage, and observe operational workflows in a cloud environment. • Develop processes to track and assess the security of servers, applications, software platforms, and websites which reside in cloud environments. • Serve as an expert in monitoring and assessing the data held in the cloud on an ongoing basis. Identify suspicious behavior, existing threats, vulnerabilities, and recommend remediations and mitigate further damage. • Serve as an expert in identifying, recommending, and implementing systems to minimize loss of critical assets. Audits and investigates sources of known losses. • Lead in maintaining compliance, discover vulnerabilities, protect sensitive data, and leverage continuous cloud monitoring and support to avoid business disruptions. • Serve as an expert analyst in threat intelligence and assist in conducting investigations, using adversary tactics, and response to attacks in the event of breach. • Serve as an insider threat analyst to identify threat actors, insider threat risks, conduct risks, investigate the data collected, to monitor any suspicious activities. • Conducts analysis, providing assessments of known insider threats and vulnerabilities discovered, and identity policy violations.
20%	**Information Security Incident Management Activities** • Serve as an expert on information security activities and governance. Lead and manage security and privacy incident response efforts. Report incidents to external entities as required. Manage privacy breach response and notification efforts as needed. Provide high-level advice and assistance to executive management on specific information security related activities and audit issues. • Work with the ISO on incident management. Logging in CDT California Compliance and Security Incident Reporting System (Cal-CSIRS). Lead and manage security privacy incident response efforts. Report and log the incidents in CDT's California Compliance and Security Incident Reporting System (Cal-CSIRS). Manage privacy breach response and notification efforts. • Research problems to provide effective IT security solutions and make recommendations for organizational improvements. Collaborate with the IT Managers to support the implementation of information security and privacy improvements. • Assist management in conducting privacy threshold analysis (PTA) and privacy impact assessments (PIA). • Monitor the Privacy email mailbox for blocked emails and respond. Maintain the blocked lists and provide a monthly report to executives. • Audit information assets which contain personal information to maintain accountability using asset management tools. • Analyze and understand the information assets and assist in creating a process to classify data and information stored on hosts, based on FIPS 199.

15%

Security Policies, Processes, Procedures, Standards, and Guidelines Activities

- Serve as an expert on information security and privacy 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.
- Lead in efforts to develop and maintain security and privacy policies to align with applicable laws, regulations, statewide policies, and CalVCB's strategic framework; assess existing policies and identify opportunities to improve alignment.
- Ensure security, privacy policies, processes, procedures, standards, and guidelines align with applicable laws, regulations, statewide policies, and CalVCB's information security and privacy policies. Coordinate efforts to ensure procedures, standards, and guidelines are disseminated to personnel.
- Research privacy laws and regulations, privacy protection controls, and information classification.

5%

MARGINAL JOB FUNCTIONS:

Other Responsibilities
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.