☒Current ☒Proposed

STATE OF CALIFORNIA
CALIFORNIA VICTIM COMPENSATION BOARD
Rev. 04/22

DUTY STATEMENT

EMPLOYEE		RPA # / JOB CONTROL #	
Vacant		23-106 / 335074	
POSITION NUMBER	CLASSIFICATION	WORKING TITLE	
040-410-1405-003	Information Technology Manager I	Information Security Officer	
DIVISION	SECTION/UNIT	CBID	WWG
Information Technology	Information Security	M01	E
WORK DAYS	WORK HOURS	TENURE	TIME BASE
Monday – Friday	8AM – 5PM	Permanent	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, 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 provide financial assistance to victims of crime and help them restore their lives. At CalVCB, we work to reduce the impact of crime of 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 job 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. 04/22) **RPA 23-106**

GENERAL STATEMENT

Under the general direction of the Chief Information Officer, the Information Technology Manager I (ITM), serves as the Information Security Officer (ISO), who develops, manages, and oversees CalVCB's information security program ensuring protection of mission critical systems and data. The ISO also operates as a high-level technical specialist responsible for the CalVCB's information security framework, architecture, security operations, and training.

The IT Manager I will also ensure that the CalVCB's Information Security and Privacy Policies are in alignment with the California Information Practices Act, as well as federal privacy laws and regulations, State Administrative Manual (SAM) Section 5300 and the Statewide Information Management Manual, Information Security Program Management Standard (SIMM 5305-A). Administratively, the ITM oversees IT budgeting, purchasing, and asset management activities.

This position will primarily provide leadership for the Information Security Engineering and Business Technology Management domains.

PERCENTAGE OF TIME SPENT	DUTIES
%	**ESSENTIAL JOB FUNCTIONS**
25%	Information Security Program Management Activities • Manage and oversee all asepects of CalVCB's information security program. • Monitor and report the implementation and compliance with State policies annually and quarterly. • Prepare confidential reports. • Conduct ongoing assessments to identify potential vulnerabilities that could threaten the security, confidentiality, and integrity of CalVCB information assets. • Identify and estimate the cost of protective measures to eliminate or reduce vulverabilities. • Participate in IT projects at the strategic and tactical levels to ensure design and deliverables align with policy, and sufficient information security resources are allocated to properly secure data and systems from cybersecurity threats.
20%	Information Security Technical Specialist Activities • Manage and report information security incidents. • Formulate, develop, and document the baseline security architecture and a sustainable target architecture aligned to the enterprise strategic management plan. • Configure, operate, and maintain security tools to identify, detect, and protect informaiton assets. • Configure, operate, and maintain security tools to respond to, and recover from security incidents and attacks. • Manage security training tools to increase enterprise security awareness, knowledge, and skills. • Compile and report results and statistics from security tools.

20%	Information Privacy Oversight Activities • Provide consultation with the programs within CalVCB to ensure staff observe standards and procedures that follow privacy and disclosure best practices. • Coordinate with regulatory authorities and the public concerning privacy issues. • Provide expert level guidance to the CalVCB's Executive Staff regarding security and privacy risks and issues, with periodic attendance and participation in various executive level meetings, as required. • Perform continuous assessment of information security and privacy programs and operations, to identify and implement improvements and efficiencies. • Provide support to develop and maintain Privacy Impact Assessments (PIA)/Privacy Threshold Assessments (PTA).
20%	General Leadership & Personnel Management Activities • As part of the IT Division senior leadership team, the ISO collaborates with the CIO, Section Chiefs, Executive staff, and Program Management on information security activities, organizational issues, governance, and strategic planning. • Provide high level advice and assistance to executive management on specific information security related activities and audit issues. • Act as project lead for complex analytical studies involving cross-functional teams. • Research problems to provide effective solutions, make recommendations for process improvements. • Provide leadership, guidance, and direction to staff on a variety of personnel related issues. • Set priorities, manage workload, monitor progress, and adjust as necessary. • Establish performance criteria and assess employee performance by conducting annual performance appraisals and probationary reports. • Meet regularly with staff and provide continual feedback and guidance. • Perform the full range of tasks related to personnel management, development, and retention.
10%	Cross Functional Activities • Coordinate information systems assessments and audits with state and federal agencies, including the California Department of Technology, the California Military Department, and other government and private organizations. • Invest in personal development through ongoing continuous research and education to maintain position related knowledge in the information security technology field with emphasis on cross-training and knowledge transfer within CalVCB IT. • Produce, formalize and maintain documentation and operational guides for security controls including but not limited to: Multi Factor Authentication, Encryption, Malware, Web Filtering, Penetration Testing, Security Information and Event Management (SIEM) Monitoring, and Data Loss Prevention. • Cross work and cross train with other IT sections and personnel as required. • Other duties as assigned.
5%	Business Technology Management Activities • Oversee and provide leadership, guidance, and direction to subordinates on IT budgeting, cost tracking and reporting, purchasing, and asset management.

DESIRABLE QUALIFICATIONS

- A Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM).
- Technical competence with configuring, operating, and maintaining information security tools.
- Deep knowledge of NIST and FIPS security standards and practices and their practical application.
- Experience with Information Technology (IT) leadership, management, and workforce planning.
- Experience with IT budgeting, cost-tracking, purchasing, and asset management.
- Experience with backup, recovery, and disaster preparedness.
- Experience with technical report writing, research, and analysis.
- Knowledge of project management concepts, terms, and methodologies.
- Knowledge of industry best practices and standards for IT systems, services, and processes
- Knowledge of functional and technical requirements and system design concepts.
- 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.