EXHIBIT A
SCOPE OF WORK

1. This Agreement is entered between the County of El Dorado (Contractor) and the California Victim Compensation Board (CalVCB), collectively known as the “parties”.

2. This Agreement will commence on July 1, 2021 or upon approval by the California Department of General Services (DGS), whichever is later, and no work shall begin before that time. This Agreement is of no effect unless approved by DGS. Contractor shall not receive payment for work performed prior to approval of the Agreement. This Agreement shall expire on June 30, 2024. The services shall be provided during the working hours of 8:00 AM through 5:00 PM, Monday through Friday, excluding State holidays. At the beginning of each fiscal year, Contractor shall provide a list of scheduled holidays for the coming year. Contractor shall obtain approval from the Contract Manager or designee prior to any temporary changes in schedule, including overtime or operating hours. The parties may amend this Agreement as permitted by law.

3. Location of Services

   A. Services shall be performed at:

County	County of El Dorado
Office	County of El Dorado District Attorney's Office
Office Location	778 Pacific Street Placerville, CA 95667

   B. Telework Option

   CalVCB allows the use of telework as a work option for Contractor’s staff when a telework agreement between the staff and CalVCB has been made, and no other means of providing the services as described in this Exhibit A, Scope of Work is available. The telework agreement must follow the hours stated in section 2 of this Exhibit A, Scope of Work. Telework means working at a worksite one or more days away from the office location stated above on a limited or permanent basis. Worksite is defined as either at home or at an alternative worksite. The worksite must allow for a secure working environment and confidential information must be secured. CalVCB reserves the right to terminate the telework agreement when it is deemed as no longer beneficial for either party.

4. All inquiries during the term of this Agreement will be directed to the representatives listed below:

CA VICTIM COMPENSATION BOARD	COUNTY OF EL DORADO
Division: Victim Compensation Division	Office: County of El Dorado District Attorney's Office
Contract Manager: Dionne Bell-Rucker	Contact: Johana Millan
Address: 400 R Street, Suite 400 Sacramento, CA 95811	Address: 778 Pacific Street Placerville, CA 95667
Phone: 916-491-3512	Phone: 530-642-5169
Email: dionne.bell-rucker@victims.ca.gov	Email: johana.millan@edcgov.us

5. Contractor shall provide to CalVCB the following services for victims of crime.

A. Data Entry Verification and Review of Applications and Bills

Enter data from applications and bills received from victims of crime for unreimbursed financial losses into CalVCB's automated claims management system. Verify and process pursuant to the statutes, regulations, policies and directives of CalVCB. The Contractor shall conduct data entry verification and review of applications and bills from the following county(ies): El Dorado, Alpine, and Lake.

B. Overpayment Processing

Should the Contractor make an error which results in an overpayment, the Contractor shall follow the processes, policies, and directives of CalVCB to correct the error made and shall collect monies owed as a result of the overpayment. Contractor shall notify Contract Manager or designee immediately upon the discovery of an error made resulting in an overpayment.

C. Emergency Expenses

Administer emergency expenses under Government Code (GC) section 13952.5, subdivision (c) pursuant to an approved Revolving Fund Agreement with CalVCB.

D. Outreach and Training

Contractor shall provide outreach and training to stakeholders and members of the public within the designated service area to the extent that such activities do not adversely affect the Contractor's ability to conduct data entry verification, review of applications and bills, or supervisory duties.

Supervisors shall spend no more than 20% of their time conducting outreach and training activities to stakeholders and members of the public. The Contractor shall obtain written authorization via email from the Contract Manager or designee at least five (5) business days prior to conducting outreach or training. The Contractor shall utilize CalVCB resource materials. At CalVCB's discretion, summary reports regarding outreach and training activities may be requested.

6. Services under this Agreement shall be performed by staff that have satisfactorily completed all required training provided by CalVCB and certified by CalVCB as qualified to perform such duties.

7. The Contractor shall only use information collected under this Agreement for services identified in this Exhibit A, Scope of Work.

8. The Contractor shall use CalVCB's automated claims management system known as the Compensation and Restitution System (Cares), to perform the services identified in this Exhibit A, Scope of Work. The Contractor shall ensure that all staff performing duties under this Agreement comply with CalVCB guidelines, procedures, directives, and memos pertaining to the use of the Cares system as stated in section 18, Exhibit D, Special Terms and Conditions.

9. Contractor shall use forms and processes produced by CalVCB to perform the services as stated in this Exhibit A, Scope of Work. Forms, letters, or other documentation created by the Contractor and intended for the public, shall be submitted in electronic form via email to the Contract Manager for review and written approval prior to use.

10. The Contractor's funded supervisory position shall conduct quality assurance reviews on applications and bills processed by staff and perform workload management duties to ensure processing timeframes are in accordance with statue and as directed by the CalVCB.

11. The Contractor shall maintain the highest customer service standards and shall ensure that applications and bills are processed accurately and efficiently, that applicants receive responses to their inquiries within two (2) business days of receipt, and are treated with sensitivity and respect when communicating verbally and in writing. CalVCB shall communicate in writing to the Contractor any compliance issues or concerns about the foregoing, and the Contractor shall respond to CalVCB within the time specified in the written communication.

12. CalVCB may, at its sole discretion, redirect workload (1) from CalVCB to a Contractor; (2) from one Contractor to another Contractor; or (3) from a Contractor to CalVCB. The Contractor may, with approval from the Deputy Executive Officer (DEO) of the Victim Compensation Division (VCD) at CalVCB or designee, establish Memorandums of Understanding (MOU) to conduct data entry verification and review of applications and bills received from other counties.

13. Hardware and Software Responsibilities

CalVCB shall not be responsible for the procurement activities for all necessary hardware and software. The Contractor shall provide necessary hardware and software to complete services as stated in this Exhibit A, Scope of Work.

EXHIBIT B
BUDGET DETAIL AND PAYMENT PROVISIONS

1. INVOICING AND PAYMENT

A. For services satisfactorily rendered, and upon receipt and approval of the services and invoices by CalVCB, CalVCB agrees to reimburse the Contractor for actual allowable expenditures incurred as specified in Exhibit B-1, Budget.

B. Invoices shall include the Agreement Number S21-010 and shall be submitted not more frequently than monthly by the 30th of each month, in arrears to:

Address: California Victim Compensation Board
Attn: Accounting
P. O. Box 1348
Sacramento, CA 95812-1348

Or by email: accountingmailbox@victims.ca.gov

C. Invoices shall be itemized and include the following information:

- County name
- Date of invoice
- Invoice Number
- Direct costs and overhead costs
- Employee fringe benefits
- Time sheets or attendance records with month/year
- Position/classification, time base, and monthly/weekly/hourly rate for all staff
- Other expenses

D. Fiscal Year Invoice Closeout

The Contractor shall submit a fiscal year closeout invoice within forty-five (45) calendar days after June 30th of each year. The final reimbursement to the Contractor shall be contingent upon the receipt and approval of the closeout invoice by CalVCB.

Fiscal Year	Closeout Invoice Due Date
FY 2021/2022	August 15, 2022
FY 2022/2023	August 15, 2023
FY 2023/2024	August 15, 2024

2. BUDGET CONTINGENCY CLAUSE

A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, CalVCB shall have no liability to pay any funds whatsoever to the Contractor or to furnish any other consideration under this Agreement and the Contractor shall not be obligated to perform any provisions of this Agreement.

B. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, CalVCB shall have the option to either terminate this Agreement with no liability to CalVCB, or offer an amendment of this Agreement to the Contractor to reflect the reduced amount.

C. Federally Funded Agreements

1) It is mutually understood between the parties that this Agreement may have been written for the mutual benefit of both parties before ascertaining the availability of congressional appropriation of funds to avoid program and fiscal delays that would occur if the Agreement were executed after that determination was made.

2) In addition to section 2(A) above, this Agreement is valid and enforceable only if sufficient funds are made available to the State by the United States Government for the fiscal years 2021-2024 for the purpose of this program. In addition, this Agreement is subject to any additional restrictions, limitations, or conditions enacted by the Congress or to any statute enacted by the Congress that may affect the provisions, terms, or funding of this Agreement in any manner.

3) The parties mutually agree that if the Congress does not appropriate sufficient funds for the program, this Agreement shall be amended to reflect any reduction in funds.

4) In its sole discretion, CalVCB may invalidate the Agreement under the 30-day cancellation clause or to amend the Agreement to reflect any reduction in funds.

3. PROMPT PAYMENT CLAUSE

Payment will be made in accordance with, and within the time specified in, GC Chapter 4.5, commencing with section 927.

4. PAYMENT PROVISIONS

A. Payments made to the Contractor are on a cost-reimbursement basis. Contractor must set forth in detail the reimbursable items, unit rates, and extended total amounts for each line item in Exhibit B-1, Budget. The following information shall be documented:

1) Identify and justify direct costs and overhead costs, including employee fringe benefits;

2) Monthly, weekly or hourly rates as appropriate and personnel classifications shall be specified, together with the percentage of personnel time to be charged to the contract, when salaries and wages are a reimbursable item;

3) Rental reimbursement items shall specify the unit rate, such as the rate per square foot; and

4) If travel is to be reimbursed, the Contractor acknowledges and understands that the rates of reimbursement for necessary travel expenses and per diem shall be set in accordance with the rates of the California Department of Human Resources (CalHR) for comparable classes and that no travel outside the State of California shall be reimbursed. Travel rates can be found at: http://www.calhr.ca.gov/employees/Pages/travel-reimbursements.aspx

B. The Contractor must obtain prior authorization by CalVCB before Contractor will be reimbursed for any purchase order or subcontract exceeding $2,500 for any articles, supplies, equipment, or services. Contractor shall submit to the Contract Manager a written request via email. The Contractor shall provide in its request for authorization all particulars necessary for evaluation of the necessity or desirability of incurring such cost and the reasonableness of the price or cost. Three competitive quotations shall be submitted or adequate justification provided for the absence of bidding.

C. In order to receive reimbursement, the Contractor shall submit a proposed budget to CalVCB for each fiscal year no later than the date indicated in the table below. The Contract Manager or designee shall provide written approval of the proposed budget(s) and any subsequent modification(s).

Fiscal Year	Date
FY 2021/2022	July 1, 2021 or upon Agreement approval by DGS, whichever is later
FY 2022/2023	March 1, 2022
FY 2023/2024	March 1, 2023

5. RECORD KEEPING

CalVCB requires the contractor to maintain books, records, documents, and other evidence pertaining to the reimbursable costs and any matching costs and expenses and to hold them available for audit and inspection by the State for seven (7) years.

6. COST LIMITATION

A. The amount of this Agreement shall not exceed $ 542,023.23.

B. For each fiscal year, CalVCB will allocate to the Contractor the following amounts:

Fiscal Year	Dollar Amount
FY 2021/2022	$ 180,674.41
FY 2022/2023	$ 180,674.41
FY 2023/2024	$ 180,674.41

7. REDUCTION OF CONTRACT AMOUNT

CalVCB reserves the right to reduce the amount in the Agreement if CalVCB's fiscal monitoring indicates that the Contractor's rate of expenditure will result in unspent funds at the end of the fiscal year or when deemed necessary.

EXHIBIT B-1
BUDGET

EXHIBIT C
GENERAL TERMS AND CONDITIONS

General Terms and Conditions (GTC 04/2017)
All documents issued under this contract incorporate the contract terms and applicable California General Terms and Conditions for non-IT services: https://www.dgs.ca.gov/OLS/Resources/Page-Content/Office-of-Legal-Services-Resources-List-Folder/Standard-Contract-Language

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

1. SETTLEMENT OF DISPUTES

   A. Any dispute concerning a question of fact arising under this Agreement that is not disposed of by mutual agreement shall be decided by CalVCB's Enterprise Operations and Services Section (EOSS) Chief, who may consider any written or verbal evidence submitted by the Contractor. The decision of the EOSS Chief, issued in writing, shall be CalVCB's final decision regarding the dispute.

   B. Neither the pendency of a dispute nor its consideration by the EOSS Chief will excuse the Contractor from full and timely performance in accordance with the terms of the Agreement.

2. TERMINATION

   A. If, after award and execution of the Agreement, the Contractor's performance is unsatisfactory, the Agreement may be terminated for default. Default is defined as the Contractor failing to perform services required by the Agreement in a satisfactory manner.

   B. CalVCB reserves the right to terminate this Agreement without cause upon thirty (30) days written notice to the Contractor, or immediately in the event of default or material breach by the Contractor.

3. PERSONNEL SERVICES AND WORKLOAD

   A. The Contractor shall submit by mail to CalVCB, in accordance with state law, a signed Statement of Economic Interests (Form 700) for each staff performing work under this Agreement who is responsible for recommending an initial eligibility or payment decision, and for each person in a supervisory position over such staff. The Form 700 must be mailed to CalVCB within five (5) business days of hiring new staff and, thereafter, must be submitted on an annual basis. The Contractor shall submit all Form 700s no later than thirty (30) calendar days from CalVCB's request each year. Upon the resignation or termination of a staff person as described in this paragraph, the Contractor shall submit a final Form 700 within ten (10) business days to CalVCB.

   B. The Contractor shall notify CalVCB when staff assigned to perform the functions of this Agreement has been absent or is expected to be absent for any reason, longer than two weeks. When staff is on leave, including vacation, sick, and annual leave, CalVCB shall reimburse the Contractor for leave accrued during that period of time if staff was performing services stated in Exhibit A, Scope of Work. Further, the Contractor agrees to provide, at CalVCB's request, documentation verifying leave accrued under this Agreement.

C. The Contractor shall ensure staff assigned to perform services under this Agreement do not:

- Participate in criminal investigations or prosecution
- Act as an agent for the collection of restitution
- Serve as a restitution specialist or victim advocate, with the exception of the director of the county victim assistance program.

D. The Contractor shall budget no more than 20%·of the salary and benefits for the director of the county victim assistance program as part of this Agreement, unless a request for additional funding is submitted to the Contract Manger via email for review and approval. Requests to increase a director's salary and benefits budget above 20% shall include the time spent per month performing training and outreach, or other duties as outlined in Exhibit A, Scope of Work and a justification as to why the duties are required.

E. The Contractor shall obtain prior written authorization from the Contract Manger before including the salaries of any other administrative staff who are not directly involved in performing the services as described in Exhibit A, Scope of Work, or the supervision of staff fulfilling functions under this Agreement in the budget.

F. Contractor shall obtain prior written authorization from the DEO of VCD or designee if staff assigned to perform services as described in Exhibit A, Scope of Work, will perform any other county functions. Should the Contractor assign a staff to perform services other than those described in Exhibit A, Scope of Work, the Contractor shall request written authorization ten (10) calendar days prior to start of the staff performing the services. CalVCB shall not reimburse the Contractor for services performed outside the scope of this Agreement or for any services rendered or performed prior to its written authorization.

G. For each staff providing services under this Agreement, the Contractor shall provide to CalVCB:

- Name
- Business address
- Telephone number
- Email
- Job title
- Description of duties
- Supervisor's Name
- Names of staff supervised, if applicable
- Other information as required by CalVCB

The Contractor shall also provide contact information for individual county victim assistance centers and advocate staff responsible for sending applications and bills directly to the Contractor. The Contractor shall update the information anytime a change is made.

H. Contractor agrees to pay Contractor staff in accordance with federal and state labor laws.

I. Requirements as described in this section 3 of Exhibit D, Special Terms and Conditions, are to be sent to:

Address: California Victim Compensation Board
Joint Powers County Liaison Unit (JPU)
P.O. Box 3036
Sacramento, CA 95812-3036

Email: Dionne.Bell-Rucker@victims.ca.gov

4. INCOMPATIBLE ACTIVITIES

A. Contractor's staff assigned to perform services for CalVCB shall not:

1) Participate in a criminal investigation or prosecution.

2) Engage in any conduct that is clearly inconsistent, incompatible, or in conflict with his or her assigned duties under this Agreement, including but not limited to, providing services that could be compensated by CalVCB.

3) Use information obtained performing services under the Agreement for personal gain or the advantage of another person.

4) Disclose any confidential information to anyone, including but not limited to, victim advocates, community-based organizations, law enforcement, prosecutors and others, unless authorized by CalVCB. Confidential information includes, but is not limited to: information about applicants, applications, crime documentation and other documents associated with applications.

5) Provide or use the name of persons or records of CalVCB for a mailing list, which has not been authorized by CalVCB.

6) Represent himself or herself as a CalVCB employee.

7) Take any action with regard to a victim compensation claim or restitution matter with the intent to obtain private gain or advantage.

8) Involve himself or herself in the handling of any claim or restitution matter when he or she has a relationship (business or personal) with a claimant, suspect, or other interested party.

9) Knowingly initiate any agreement with a person for whom restitution may be sought, or person against whom restitution may be collected.

B. All confidential information obtained during the performance of this Agreement shall be held in strict confidence and shall not be provided to persons not authorized to receive the information.

C. It shall be the Contractor's responsibility to ensure that all staff assigned to provide services under this Agreement is made aware of and abides by these provisions as stated in this section 4 of Exhibit D, Special Terms and Conditions. If an assigned staff is unwilling or unable to, or fails to abide by these provisions, the staff shall no longer be assigned to perform services in this Agreement and CalVCB shall not reimburse Contractor for expenditures incurred, including staff salary.

5. PERFORMANCE ASSESSMENT

A. CalVCB shall assess and evaluate the Contractor's performance in a manner consistent with methods currently in place for CalVCB staff performing the same type of services. CalVCB shall monitor performance of services under this Agreement and periodically report performance evaluations to the Contractor.

B. CalVCB shall set production and accuracy expectations or goals for services to be performed as described in Exhibit A, Scope of Work, for staff, leads and supervisors. Those expectations may include, but are not limited to, time frames for the completion of work, amount of work to be completed within given timeframes and standards for the quality of work to be performed. At the inception of Agreement start date and periodically thereafter, CalVCB shall provide written notice of production and accuracy expectations to the Contractor. If the Contractor fails to achieve production and accuracy expectations set by CalVCB as set forth in the written notice, CalVCB reserves the right to implement a Corrective Action Plan (CAP) for the office and/or staff, reduce the amount of the Agreement, terminate the Agreement as described in section 2 of Exhibit D, Special Terms and Conditions, or remove the staff from the Agreement.

C. CalVCB reserves the right to implement a CAP and revoke Cares access to staff whose production and accuracy is consistently poor or below average based on the performance criteria identified by CalVCB or who do not comply with the provisions of this Agreement. Any staff whose access has been revoked shall no longer be authorized to perform services as described in Exhibit A, Scope of Work, and the salary of that staff no longer reimbursable by CalVCB. Contractor may replace staff in accordance with section 3 of Exhibit D, Special Terms and Conditions.

D. CalVCB requires supervisors to utilize production, aging and workload reports, provided by CalVCB, to maintain the level of production as outlined by CalVCB. The Contractor shall inform the Contract Manager or designee of performance or other staffing issues immediately upon identification and implement a CAP for immediate improvement of the area of concern.

6. OPERATING EXPENSES

A. The Contractor may charge expenses to various line-item allocations as part of its operating expenses, including but not limited to: rent, utilities, postage, and telephone. Such expenses are generally identified as “direct costs”. The Contractor shall ensure that expenses that are classified as “direct costs” are not also included in the “indirect cost” or “overhead” categories. Indirect costs are those costs that are incurred for a common or joint purpose or a cost that is not readily assignable to a specific operating expense line-item. CalVCB reserves the right to deny any expenses that are deemed ineligible by the State.

B. The Contractor shall submit, upon CalVCB’s request, a copy of the indirect cost allocation plan demonstrating how the indirect cost rate was established. All costs included in the plan shall be supported by formal accounting records, which substantiate the propriety of such charges.

C. The total amount budgeted for operating expenses, including direct and indirect expenses, shall not exceed 18% of the entire amount of this Agreement.

D. The Contractor shall submit requests to the Contract manager or designee via email for review and prior written approval of any budget modification for line items under the operating expense category such as an increase to rent or offsetting savings from one line item to another.

7. TRAINING RELATED REIMBURSEMENT

Contractor shall obtain prior approval from CalVCB for the location, costs, dates, agenda, instructors, instructional materials, and attendees at any reimbursable training seminar, workshop or conference and over any reimbursable publicity or educational materials to be made available for distribution. The Contractor shall be required to acknowledge the support of CalVCB when publicizing the work under the Agreement in any media.

All such costs must be disclosed in Exhibit B-1, Budget and included in the amount as stated in section 6 of Exhibit B, Budget Detail and Payment Provisions. Contractor must complete and submit to the Contract Manager or designee, a Training Request Form (Attachment 1). Approval for reimbursement for the requested training is at the discretion of CalVCB.

8. TRAVEL REIMBURSEMENT

The Contractor shall obtain written authorization via email from the Contract Manager or designee at least five (5) business days prior to any in-state travel for which the Contractor intends to seek reimbursement. Any reimbursement for necessary travel and per diem shall be at the rates currently in effect as established by CalHR. Current travel rates can be found at: http://www.calhr.ca.gov/employees/Pages/travel-reimbursements.aspx. No out-of-state travel is authorized under this Agreement.

9. MOVING

CalVCB shall not reimburse Contractor any costs associated with the relocation of staff performing services as described in Exhibit A, Scope of Work. Contractor shall notify CalVCB prior to relocation. Notification shall include the following:

- Name of Staff
- New address, including room number
- Contact person, including title, address and phone number

10. BUILDING AND CONSTRUCTION

Payments are not permitted for construction, renovation, alteration, improvement, or repair of privately owned property when such work would enhance the value of the property to the benefit of the owner.

11. INFORMATION TECHNOLOGY EQUIPMENT AND SOFTWARE

A. The Contractor is responsible for the purchase, configuration, installation, and support of all computer equipment used for CalVCB data processing activities. CalVCB will reimburse the Contractor for Information Technology Equipment in accordance with section 12 of Exhibit D, Special Terms and Conditions.

B. For software purchased and reimbursed under this Agreement, Contractor shall certify that it has appropriate systems and controls in place to ensure that State funds are not used to acquire, operate, or maintain computer software in a manner that does not comply with applicable copyrights.

C. Contractor shall install and maintain current anti-virus software, security patches, and upgrades on all computing devices used during the course of the Agreement. Contractor shall apply appropriate end point protection, data encryption, and data loss prevention technologies employed by the local entity.

D. All machines must be configured to accept and apply software and security updates for all software installed on the device. This includes the operating system, applications, programs, utilities, and anti-virus software.

E. CalVCB reserves the right to ensure Contractor’s equipment connecting to CalVCB systems are patched, used and operated in a manner consistent with State policy and the terms of this Agreement.

F. To use CalVCB applications effectively, all personal computing devices shall meet the following minimum hardware standards:

- Intel 4th Generation Multi-Core i7 Processor
- 8 GB Ram
- 500 GB Hard Drive
- Network Port
- USB Port(s)
- 24" Flat Screen Monitor
- USB Keyboard
- USB Mouse or Trackball

G. The Contractor's Information Technology Department must notify by email CalVCB's Information Technology Division at helpdesk@victims.ca.gov and Contract Manager or designee of any change of a public internet protocol (IP) address within one (1) business day of the change.

12. STATE-PURCHASED OR STATE-FINANCED PROPERTY

A. Purchasing of Equipment

The Contractor shall obtain prior written authorization from CalVCB for the acquisition of all equipment over $2,500, including but not limited to, modular furniture and IT equipment, even though funding may have been previously requested and made part of the budget. Splitting procurement to circumvent this requirement may result in the reimbursement request not being allowed. CalVCB reserves the option of not reimbursing the Contractor for equipment purchases that are not approved in writing prior to purchase. The Contractor shall submit the County Purchase Request Form (Attachment 2) to the Contract Manager or designee for approval.

B. Asset Identification

Equipment reimbursed under this Agreement over $500 or those that contain data regardless of the dollar value are to be identified, inventoried, and affixed with a CalVCB issued asset tag. Contractor shall submit to the Contract Manager or designee a CalVCB Asset Identification Form (Attachment 3) to obtain an asset tag and once issued, must affix the asset tag to the equipment.

C. Inventory

CalVCB reserves title for State-purchased or State-financed property, which is not fully consumed in the performance of this Agreement. All equipment reimbursed under this Agreement shall be specified, remain the property of CalVCB and bear asset tags supplied by CalVCB. The Contractor shall prepare and submit to CalVCB by July 30th of each year, an inventory listing of equipment reimbursed by CalVCB using the CalVCB County Inventory Form (Attachment 4). The completed form shall be submitted by e-mail to the assigned JPU analyst.

Contractor must comply with the policies and procedures regarding State-owned property accounting set forth in the State Administrative Manual sections 8640, et seq. Prior to the disposal or surplus of equipment, the Contractor shall obtain approval from CalVCB's Business Services Unit by contacting the assigned JPU analyst to initiate the process. CalVCB reserves the right to request at any time during the Agreement period a current and complete inventory listing and to remotely access, for audit purposes, all equipment purchased and reimbursed under this Agreement.

In the event of termination of this Agreement, Contractor shall return property listed in the CalVCB County Inventory Form to CalVCB.

13. CONFIDENTIALITY OF RECORDS

A. All financial, statistical, personal, technical and other data and information relating to the State's operations which are designated confidential by the State and made available to the Contractor in order to carry out this Agreement, or which become available to the Contractor in carrying out this Agreement, shall be protected by the Contractor from unauthorized use and disclosure through observance of the same or more effective procedural requirements as applicable to the State. This includes the protection of any extractions of CalVCB's confidential data for another purpose. Personally Identifiable Information (PII) shall be held in the strictest confidence, and shall not be disclosed except as required by law or specifically authorized by CalVCB, refer to the Information Security Policy (Attachment 5).

B. CalVCB's Custodian of Records shall be notified when an applicant or applicant's representative requests a copy of any document pertaining to the claimant's file. The Contractor shall not disclose any document pursuant to any such request unless authorized to do so by CalVCB's Custodian of Records or Legal Division.

CalVCB's Legal Section is to be immediately notified of any request made under the Public Records Act (PRA) (GC sections 6250, et. seq.) or the Information Practices Act (IPA) (Civil Code sections 1798, et seq.) for information received or generated in the performance of this Agreement. No records shall be disclosed pursuant to any request unless authorized by CalVCB's Legal Section.

C. The Contractor shall be responsible for any unauthorized disclosure by Contractor staff performing duties under this Agreement and shall indemnify, defend and hold harmless the State, its officers, agents and employees from any and all claims, losses, damages, penalties, fines, and attorney fees resulting from the unauthorized disclosure of CalVCB records by such staff.

D. The Contractor shall ensure all staff performing services under this Agreement are informed of and comply with the requirements in this section 13 of Exhibit D, Special Terms and Conditions. Contractor shall provide to CalVCB, at the time of the Agreement start date, a signed CalVCB Confidentiality Statement (Attachment 6) from each staff and thereafter, annually by July 1st of each year. For new staff, Contractor shall submit within ten (10) business days from the start

date, a signed Confidentiality Statement to CalVCB. Signed Confidentiality Statements should be sent to:

Address: California Victim Compensation Board
Joint Powers County Liaison Unit (JPU)
P.O. Box 3036
Sacramento, CA 95812-3036

Email: Dionne.Bell-Rucker@victims.ca.gov

14. SUBPOENAS

A. The Contractor is not the Custodian of Records for any of the materials it creates or receives pursuant to this Agreement. The Contractor shall post a notice in its receiving department or other appropriate location stating that all subpoenas for CalVCB records must be personally served at:

California Victim Compensation Board
400 R Street, 5th Floor
Sacramento, CA, 95811
Attn: Legal Section

B. The Contractor must notify anyone attempting to serve a subpoena of this requirement. The Contractor may also contact CalVCB's Legal Section at 916-491-3605 for further assistance.

C. In cases where documents are being subpoenaed, the Contractor shall provide CalVCB with original and complete claim documents upon request. The Contractor shall submit the original claim documents in the most expedient manner necessary to meet the time constraints of the subpoena, including the use of overnight express mail.

15. RETENTION OF RECORDS

A. For the purpose of determining compliance with GC section 8546.7, the Contractor and any Subcontractors shall maintain all books, documents, papers, accounting records, and other evidence pertaining to the performance of the Agreement, including but not limited to, the costs of administering the Agreement and documents as stated in section 5 of Exhibit B, Budget Detail and Payment Provisions. All parties shall make such materials available at their respective offices at all reasonable times during the Agreement period and for a minimum of seven (7) years from the date the record is created. The State, the State Auditor, or any duly authorized representative of the Federal government having jurisdiction under Federal laws or regulations (including the basis of Federal funding in whole or in part) shall have access to any books, records, and documents of the Contractor that are pertinent to the Agreement for audits, examinations, excerpts, and transactions, and copies thereof shall be furnished if requested.

B. The Contractor shall retain all hard copies of applications and bills entered into Cares for one year from the date the document is received and dispose in accordance with laws, rules and State policies (GC section 1623). The Contractor shall retain soft copies until it has been confirmed the documents have been uploaded into Cares.

16. SUBCONTRACTORS

Nothing contained in this Agreement or otherwise, shall create any contractual relation between CalVCB and any subcontractors, and no subcontract shall relieve the Contractor of its responsibilities and obligations hereunder. The Contractor agrees to be as fully responsible to CalVCB for the acts and omissions of its subcontractors and of persons either directly or indirectly employed by any of them as it is for the acts and omissions of persons directly employed by the Contractor. The Contractor's obligation to pay its subcontractors is an independent obligation from CalVCB's obligation to make payments to the Contractor. As a result, CalVCB shall have no obligation to pay or to enforce the payment of any monies to any subcontractor.

17. REGULATIONS AND GUIDELINES

All parties agree to abide by all applicable federal and state laws and regulations and CalVCB guidelines, procedures, directives, policies and memos as they pertain to the performance of this Agreement.

18. COMPLIANCE WITH CALVCB POLICY

A. The Contractor shall ensure that all staff assigned work related to this contract review and comply with the requirements of CalVCB policies, including:

- Information Security Policy (Attachment 5)
- Information Systems Security and Confidentiality Acknowledgment (Attachment 7)
- Fraud Policy (Attachment 8)
- Password Policy (Attachment 9)
- Privacy Policy (Attachment 10)
- Acceptable use of Technology Resources (Attachment 11)

B. On July 1st of each year, JPU shall provide copies to the Contractor of the policies along with an Acknowledgement of Policies Form (Attachment 12). Contractor shall have each staff performing services under this Agreement sign the form and forward all signed forms to JPU within 30 days of receipt.

19. OWNERSHIP OF WORK PRODUCT AND DATA

A. All work product as a result of the work performed by the Contractor under this Agreement, shall be owned by CalVCB and shall be considered works made for hire by the Contractor to CalVCB.

B. All intellectual property rights, ownership and title to all reports, documents, plans, and specifications produced as part of this Agreement will automatically be vested in CalVCB and no further agreement will be necessary to transfer ownership to CalVCB. The Contractor shall furnish CalVCB all necessary copies of data needed to complete the review and approval process.

20. STATE-OWNED DATA – INTEGRITY AND SECURITY

A. Contractor shall comply with the following requirements to ensure the preservation, security, and integrity of State-owned data on portable computing devices and portable electronic storage media:

1) Encrypt all State-owned data in transit and where existing technology enables encryption at rest, stored on portable computing devices and portable electronic storage media. Data encryption shall use cryptographic technology that has been tested and approved against exacting standards, such as Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules.

2) Encrypt, as described above, all State-owned data transmitted from one computing device or storage medium to another.

3) Maintain confidentiality of all State-owned data by limiting data sharing to those individuals contracted to provide services on behalf of the State, and limit use of State information assets for State purposes only.

4) Notify the Contract Manager within 24-hours of any actual or attempted violations of security of State-owned data, including lost or stolen computing devices, files, or portable electronic storage media containing State-owned data.

5) Advise the owner of the State-owned data, the CalVCB Information Security Officer, and the CalVCB Chief Information Officer of vulnerabilities that may present a threat to the security of State-owned data and of specific means of protecting that State-owned data.

B. Contractor shall use the State-owned data only for State purposes under this Agreement.

C. Contractor shall not transfer State-owned data to any computing system, mobile device, or desktop computer without first establishing the specifications for information integrity and security as established for the original data file(s).

D. The Contractor's staff assigned to perform services for CalVCB must adhere to the following provisions. Staff shall NOT:

- Attempt to access the Cares application from any location other than their assigned work location. Remote access is only permitted with prior written approval from the DEO of VCD or per an approved telework agreement.

- Share individual login ID and password with anyone else.
- Allow their computer to remember a password to the Cares application.
- Walk away from their computer without locking the screen (Ctrl+Alt+Delete}.
- Leave documents with PII unattended on printers or fax machines, or in cubicles, offices or conference rooms.
- Visit untrusted websites or open any attachments or links from untrusted email.
- Uninstall or disable anti-virus software and automatic updates.
- Install any unauthorized or unlicensed software.
- Plug a mobile phone, personal USB drive or other peripheral device into the network system or desktop computer.
- Disclose any PII information to unauthorized users.
- Send any PII via email. Staff should use application numbers, bill numbers and initials only. Staff should use encrypted email if they must send email containing PII.

Training Request

ATTACHMENT 1

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

Participant Information

Participant Name | Classification | Work Phone

Supervisor Name | Section

Course Information *Training Course Description Must Be Attached*

Class Title | Date Choice | Time

Provider | Course ID

☐ Enroll in next available class

Total Hours

Category: ☐ In Service ☐ Out Service

Justification

☐ Job Required *Training designed to assure adequate performance in a current assignment*

☐ Job Related *Of direct value to increasing proficiency in current job*

☐ Career Related *Related to career goals and self-development; also befits the department's or the state's mission*

☐ Upward Mobility *Helps prepare employees in designated upward mobility classifications for career movement*

How will this Training Benefit the Employee?

Expenses

Tuition/Fees $

Books/Supplies $

Other $

Total $

Agreement Number | Fiscal Year

Required Approvals

Note: Deputy Executive Officer / Executive Officer signature is required only for outside or online training. Include a copy of the course description (except for internal, CalHR and CPSHR trainings).

Participant Signature | Date

Supervisor' Signature | Date

Contract Manager Signature | Date

Deputy Executive Officer
Victim Compensation Division | Date

COUNTY PURCHASE REQUEST FORM

The following information must be provided in order for authorization to be granted for the purchase of equipment through the County's Agreement. As stated in the Agreement, **equipment purchases over $2,500 must be justified by the requesting County and approved by CalVCB**. If the request is not approved by CalVCB, the purchase will not be authorized for reimbursement through the Agreement. **A separate form must be completed for each piece of equipment being requested.**

1. COUNTY CONTACT INFORMATION

County:	**Contract Number:**	**Fiscal Year Funded:**
Contact Name:	**Address:**	**Phone Number:**
Email:		

2. EQUIPMENT REQUEST

Submission of this form is not a guarantee of equipment approval. CalVCB's Joint Powers County Liaison Unit (JPU) Analyst and Business Services Unit (BSU) Analyst will verify the request and make recommendations based on appropriateness and pricing. Alternatives may be recommended. Incomplete forms will be returned to the County.

Note: Acquisition of an equipment maintenance plan is the responsibility of the County and may be reimbursed through the Agreement.

Equipment Type:	**Make:**	**Model:**	**Cost:**
Software: (e.g., Windows 7, Microsoft Office Suite)			**Cost:**
Equipment Maintenance Plan: (describe terms/pricing)			**Cost:**
Reasonableness of the price or cost: (obtain three competitive quotes or provide adequate justification for the absence of bidding)			

3. PURCHASE JUSTIFICATION

Explain in full detail why this equipment is needed (replacing equipment that is over 5 years old, ongoing equipment performance issues, additional staff, etc.). You may be contacted by the JPU Analyst to provide additional information.

4. COUNTY AUTHORIZATION

By signing this form, the County Coordinator/Supervisor agrees that the information provided is accurate and true, and that the equipment/software is necessary to conduct State business. The Coordinator/Supervisor is also accepting responsibility to ensure that upon receipt, the asset tag provided for this equipment will be properly affixed to the equipment.

County Coordinator/Supervisor Signature:	**Date:**

5. PURCHASE APPROVAL

If the purchase is approved, a fully executed copy of the County Purchase Request Form will be returned to the County Contact (see Page 2). The County may then proceed with their equipment purchase. Carefully review the approval as alternative equipment may have been authorized.

NOTE: Equipment reimbursed under the County's Agreement over $500 or those that contain data regardless of the dollar value are to be identified, inventoried, and affixed with a CalVCB issued asset tag. County shall submit to the Contract Manager or designee a CalVCB Asset Identification Form to obtain an asset tag and once issued, must affix the asset tag to the equipment.

COUNTY PURCHASE REQUEST FORM

For CalVCB Staff Use Only:		
The JPU Analyst is responsible for determining if the equipment/software is necessary for the County to conduct State business, and will also ensure that the form is complete, accurate, and contains the appropriate signature. The JPU Analyst will serve as the liaison between the County Contact and the BSU Analyst for clarifying or resolving any issues. Upon review/approval by the JPU Analyst and the Contract Manager, the form will be forwarded to BSU for further review and processing.		
JPU Analyst Comments:		
This request is: ☐ **Approved** ☐ **Denied**	**JPU Analyst Name:**	**Date:**
Contract Manager's Signature (required)	**Signature:**	**Date:**
The BSU Analyst is responsible for determining if the equipment requested is available through State contracts, best pricing and/or quotes obtained, etc.		
BSU Approval / Comments (include Approved Changes or Denial details in this section)**:**		
This request is: ☐ **Approved** ☐ **Approved w/Changes** ☐ **Denied**		**Approved by (BSU Analyst):**
BSU Manager's Signature (required)	**Signature:**	**Date:**

COUNTY PURCHASE REQUEST FORM

INSTRUCTIONS AND RESPONSIBILITIES

County Staff Responsibilities – Request

1. County staff will complete each section of the County Purchase Request Form and obtain County authorization.
2. The County Staff will then submit the form to their assigned JPU Analyst.

JPU Analyst Responsibilities – Review

1. JPU Analyst reviews form to verify it is completed correctly and that sufficient funds are available.
   - If the form is not filled out correctly, the form will be returned to the County Staff with instructions on how to proceed (i.e., complete cost, provide justification, etc.).
2. Contract Manager will either sign and approve the form, or deny the request and return the form to the County Staff with an explanation of the denial.
3. If approved, JPU Analyst will send the signed, approved form to BSU for further processing.

BSU Staff Responsibilities – Process

1. BSU Analyst will verify the equipment/cost and accept or make recommendations based on appropriateness and pricing. If the request is acceptable, the BSU Manager will sign and approve the form.
   - If the form is not filled out correctly, BSU Analyst will note the necessary changes needed and return the form to the JPU Analyst.
2. BSU Analyst will note on the form whether Approved, Approved w/Changes, or Denied. Changes or reason for denial will be noted on the form.
3. BSU Analyst will make a copy of the form and return the signed copy to the JPU Analyst for processing.

JPU Analyst Responsibilities – Status

1. The JPU Analyst will notify the County of the status of the request, and if it has been approved, to proceed with their purchase.

County Staff Responsibilities – Asset/Inventory

1. For equipment over $500 or those that contain data regardless of the dollar value, once received by the County Staff, equipment is to be identified, inventoried, and affixed with a CalVCB issued asset tag.
2. County staff will complete a State Asset Identification Form and submit to their assigned JPU Analyst within 10 business days.
3. An asset tag(s) will be sent from CalVCB to the County Staff and once received, the County Staff will affix the asset tag(s) to the equipment.

Annual Inventory: County Staff must submit a completed County Inventory Form which lists equipment reimbursed under the County Agreement over $500 or those that contain data regardless of the dollar value. This form must be completed and sent to the assigned JPU Analyst by July 30th of each year.

CalVCB Asset Identification Form

As required by the State Administrative Manual and the County Agreement, equipment reimbursed under the County Agreement over $500 or those that contain data regardless of the dollar value are to be identified, inventoried, and affixed with a CalVCB issued asset tag. To comply with these requirements, the County must complete the information provided below.

Upon completion, a copy of this form must be emailed to your assigned Joint Powers County Liaison Unit (JPU) Analyst.

County Name	Agreement Number	Address
County Contact Name	**Phone Number**	**Email Address**

ASSET INFORMATION (To be completed by the County; use Page 2 for additional items)	
Asset Type	
Location/Address	
Make/Model	
Serial Number	

COUNTY ACKNOWLEDGEMENT

A complete accounting of assets and corresponding asset tags must be provided to CalVCB by July 30th of each fiscal year. County must use the CalVCB County Inventory Form provided with their Agreement to account for and report assets reimbursed with CalVCB funds over $500 or those that contain data regardless of the dollar value. The County Coordinator/ Supervisor understands and accepts responsibility for submission of a complete and accurate CalVCB County Inventory Form for the current fiscal year.

By signing below, you acknowledge that asset tags have been properly affixed to equipment reimbursed with CalVCB funds, and that an accounting of all assets will be reported by July 30th of each fiscal year, as indicated above:

County Coordination/Supervisor (required):	Date:

ASSET TAG

Asset Tag(s) Provided to JPU Analyst By:		Asset Tag(s) Sent to County By:	
Business Services Unit or Information Technology Analyst:	Date:	JPU Analyst:	Date Sent:

Once the purchase is completed, CalVCB's BSB/ITD staff will update its asset management system to include the equipment purchased for the County. An asset tag(s) will be assigned and sent to the County by the CRC/JP Analyst identified above. Upon receipt, the County must properly affix the asset tag(s) provided below to the equipment.

Asset Tag Number **To be provided by CalVCB**	

ASSET INFORMATION	
Asset Type	
Location/Address	
Make/Model	
Serial Number	
Asset Tag Number **To be provided by CalVCB**	ASSET TAG

ASSET INFORMATION	
Asset Type	
Location/Address	
Make/Model	
Serial Number	
Asset Tag Number **To be provided by CalVCB**	ASSET TAG

ASSET INFORMATION	
Asset Type	
Location/Address	
Make/Model	
Serial Number	
Asset Tag Number **To be provided by CalVCB**	ASSET TAG

ASSET INFORMATION	
Asset Type	
Location/Address	
Make/Model	
Serial Number	
Asset Tag Number **To be provided by CalVCB**	ASSET TAG

ATTACHMENT 4

CalVCB County Inventory Form

In accordance with the California Victim Compensation Board (CalVCB) Agreement with the County (Contractor), the CalVCB County Inventory Form must be completed and returned to CalVCB by July 30th of each year.

Please complete all requested information. The only assets to be inventoried on this form are those purchased and reimbursed by CalVCB under the Agreement over $500 or those that contain data regardless of the dollar. Contractor must comply with the policies and procedures regarding State-owned property accounting set forth in the State Administrative Manual section 8640, et seq. For disposal or surplus of equipment, the Contractor must obtain approval from CalVCB's Business Services Unit by contacting the assigned Joint Powers County Liaison Unit (JPU) analyst to initiate the process. Return the completed form to the assigned JPU analyst.

County Name	CalVCB Agreement Number	Date	Address	Contact Information
				Name:
				Phone Number:
				Email Address:

Asset Inventory

Asset Type	Location	Serial Number	Model	Manufacturer	Asset Tag #	Comments

For additional assets, please include on a separate document using the same format as this form.

Information Security Policy

Memo Number: 17-008
Date Issued: 1/1/17
Supersedes: 15-001
Effective Date: Immediately
Expires: Indefinite
Issued By: Information Technology Division

Purpose

The Victim Compensation Board's (CalVCB) Information Security Policy defines the rules for information security that apply to our business activities. This Policy also provides a foundation for additional practices and standards that will more specifically communicate CalVCB rules related to information security.

Information Security Program

The CalVCB has established an Information Security Program to protect the confidentiality, availability, integrity, and privacy of CalVCB information and supporting assets. The Information Security Program provides an integrated set of requirements that complement the CalVCB strategic goals and securely achieves its objectives and priorities.

Responsibility

The Information Security Officer (ISO) is responsible for developing, implementing, and operating the Information Security Program. The ISO reports directly to the CalVCB ITD Chief Information Officer.

The ISO will develop and implement policies, practices, and guidelines that protect the confidentiality, availability, and integrity of all CalVCB information and supporting assets. The ISO also promotes information security awareness, measures adherence to information security policies, and coordinates the response to information security incidents.

The ISO chairs the Information Security Advisory Committee that includes members representing all CalVCB divisions. The Information Security Advisory Committee is responsible

for reviewing, advising, and recommending approval of information security practices and standards.

The Information Technology Division is responsible for the implementation and administration of CalVCB information security policies, practices, and guidelines for all CalVCB information systems and networks.

All CalVCB employees, consultants, and contractors are responsible for protecting CalVCB information assets and complying with CalVCB information security policies, practices, and guidelines. All CalVCB employees, consultants, and contractors are also responsible for reporting any suspected or known security violations or vulnerabilities to the ISO.

Compliance

All CalVCB employees, consultants, and contractors must comply with CalVCB information security policies, practices, and guidelines.

Failure to comply with CalVCB information security policies, practices, and guidelines by State employees may result in disciplinary action up to, and including, termination of State employment.

Failure to comply with CalVCB information security policies, practices, and guidelines by consultants or contractors may result in punitive action up to, and including, termination of their contract.

In some cases, the failure to comply with CalVCB information security policies, practices, and guidelines may result in additional civil and criminal penalties.

Compliance of CalVCB divisions and offices with CalVCB information security policies, practices, and guidelines must be enforced by the supervisors and managers of these divisions and offices. The CalVCB overall compliance with information security policies, practices, and guidelines will be monitored by the ISO.

Risk Management

The CalVCB will identify and mitigate risks to the confidentiality, availability, and integrity of CalVCB information assets. Information security risks must be reported to the owner of the information or the information system asset and the owner of that asset will ultimately determine the impact of the risk and the appropriate mitigation approach.

The ISO operates the Information Security Risk Management program. Under this program, the ISO participates in the development of new information systems and periodically assesses existing information systems to identify and mitigate information security risks. The ISO works with the appropriate CalVCB divisions and offices to determine the impact of the risk, identify the appropriate mitigation activities, and monitor the successful completion of the mitigation activities.

Life Cycle Planning

The CalVCB will address information security as part of new projects involving major business activities or significant enhancements to existing business.

Projects will comply with all applicable information security policies and practices, and include provisions for the effective implementation and administration of the information security processes required for compliance.

Awareness and Training

The CalVCB maintains a mandatory information security awareness program. The ISO will ensure that the appropriate information security awareness training is provided to all CalVCB employees, consultants, and contractors.

Physical Security

The CalVCB safeguards its business areas and resources to protect and preserve the availability, confidentiality, and integrity of the department's information assets. Only authorized individuals are granted physical access to sensitive CalVCB business areas.

Contingency and Disaster Preparedness

The CalVCB Business Services Section ensures that the CalVCB has sufficient plans, resources, and staff to keep critical CalVCB business functions operating in the event of disruptions.

Contingency plans must be tested at a frequency sufficient to ensure that they will work when needed.

Incident Handling

The CalVCB ISO implements practices to minimize the risk associated with violations of information security and ensure timely detection and reporting of actual or suspected incidents or violations.

All CalVCB employees, consultants, and contractors are responsible for reporting any suspected or confirmed security violations and incidents in a timely manner. The CalVCB investigates information security violations and incidents and refers them to state and federal authorities when appropriate.

Identification and Authentication

All users are individually identified to the information system(s) they use. Their identity is verified in the system by using information that is only known by the individual user and the system. The user and the system will protect this verification information with sufficient care to prevent its disclosure and ensure its integrity.

The identification and verification process must be strong enough to establish a user's accountability for their actions on the information system.

Access Control

Access to all CalVCB information systems and information assets is controlled and the owner of each system or information asset must approve all user access. Users are provided access to only those systems and information assets required to perform their current CalVCB duties.

The CalVCB information systems must have the capability to restrict a user's access to only information and/or functions necessary to perform their CalVCB duties.

Audit Trail

All information system activities are subject to recording and routine review. Audit trail records must be sufficient in detail to facilitate the reconstruction of events if a compromise or malfunction occurs.

Audit trail records must be provided whenever access to a CalVCB information system is either permitted or denied; or whenever confidential or sensitive information is created or modified.

Audit trail records are created and stored with sufficient integrity and duration to hold a user accountable for their actions on a CalVCB information system.

Data Ownership

All information assets have a Data Owner who is assigned by CalVCB management. The Data Owner is responsible for authorizing access to the information, assignment of custody for the information, classifying the information, and approving any contingency plans affecting the information.

Information Classification

All CalVCB information assets are classified by their Data Owner according to the confidentiality of the information and its importance to CalVCB operations. In addition to any classification of information required for business purposes, the classification identifies if the information is confidential or subject to release as a public record as required by law. It also identifies information critical to the continuance and success of CalVCB operations.

Information System Security Practices

All CalVCB information systems and information system infrastructure elements will have specific practices, guidelines, and procedures that govern their operation relative to information security. All CalVCB information systems and information system infrastructure elements will conform to these practices, guidelines, and procedures unless the ISO has approved a specific exception.

Authority

- Government Code sections 19572 and 19990
- State Administrative Manual (SAM) sections 5300 through 5365.3
- Government Code section 8314
- Applicable employee Memoranda of Understanding
- State Information Management Manual (SIMM)

Contact

For any questions about this Policy, please contact your immediate manager/supervisor or the ISO by e-mail at InfoSecurityandPrivacy@victims.ca.gov.

Distribution List

All CalVCB staff

CalVCB Confidentiality Statement

Purpose of Confidentiality Statement

It is the policy of the Victim Compensation Board (CalVCB) that all computerized files and data that contain CalVCB client information, as well as all information and documents associated with such files and data, are "confidential" and shall not be disclosed except as required by law or specifically authorized by CalVCB. I also acknowledge that it is the policy of CalVCB to ensure that all information is secured as set forth in the CalVCB Information Security Policy, Memo number 06-00-003 and that all CalVCB employees and contractors must respect the confidentiality of CalVCB data by not disclosing any files or data accessible to them through their employment, contract, or affiliation with CalVCB.

State Employees and Contractors

Initial each section.

I, _____ agree to protect confidential information in the following ways:

- Access, inspect, use, disclose, or modify information only to perform job duties.
- Never access, inspect, use, disclose, or modify information, including my own, for curiosity, personal gain, or any non-CalVCB business related reason.
- Never attempt to access, use, disclose, or modify information, including my own, for any non-CalVCB business or personal reason.
- Secure confidential information in approved locations and dispose of confidential information or confidential materials using the confidential destruction receptacle. Not destroy any original copies of information submitted to CalVCB without prior authorization from the Executive Officer, Deputy Executive Officer, or Legal Counsel.
- Log off of computer access to CalVCB data and information when not using it.
- Never remove confidential information from my work site without prior authorization from the Executive Officer, Deputy Executive Officer, or Legal Counsel.
- Never disclose personal information regarding anyone other than the requestor unless authorized to do so by the Executive Officer, Deputy Executive Officer, or Legal Counsel. "Personal Information" means any information that identifies or describes an individual, including but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, or statements made or attributed to the individual.

- Never disclose any information related to a victim compensation application, including whether an individual has filed a CalVCB application, unless it is under the following circumstances:
    1. The request for information is from an applicant or the applicant's authorized representative regarding his or her own application,
    2. The disclosure is for the purpose of verifying claims and the applicant has provided a signed authorization to release information, or
    3. Are authorized to disclose the information by the Executive Officer, Deputy Executive Officer, or Legal Counsel.
- Never release a copy of a law enforcement report to any individual, including a CalVCB applicant. Law enforcement reports include, but are not limited to, reports by police, CHP, sheriff departments, DOJ, FBI, Child Protective Services, and the Department of Social Services.
- Never disclose a Felon Status Verification Request completed by DOJ to any individual outside of CalVCB.
- Never disclose any other information that is considered proprietary, copyrighted, or otherwise protected by law or contract.
- Inform the CalVCB Public Information Officer immediately of any request made under the Public Records Act (Gov. Code, § 6250 et. seq.).
- Inform a server of a subpoena that the subpoena shall be personally served on CalVCB at 400 R Street, 5th Floor, Sacramento, CA, 95811, Attn: Legal Office. Contact the CalVCB Legal Office at 916-491-3605 regarding any subpoena received by the Board.
- Notify the CalVCB Information Security Officer immediately if a suspected security incident involving the data occurs.

I, _____ acknowledge that as a state employee or individual performing work pursuant to a contract with CalVCB, I am required to know whether the information I have been granted access to is confidential and to comply with this statement and the CalVCB Information Security Policy, Memo Number 06-00-003. If I have any questions, I will contact CalVCB's Legal Office or Information Security Officer.

I, _____ acknowledge that the unauthorized access, inspection, use, or disclosure of confidential information is a violation of applicable laws, including but not limited to, the following: Government Code sections 1470 et seq, 6254.17, and 19990(c), Civil Code section 1798 et seq., and Penal Code section 502. I further acknowledge that unauthorized access, inspection, use, disclosure, or modification of confidential information, including my own, or any attempt to engage in such acts can result in:

- Administrative discipline, including but not limited to: *reprimand, suspension without pay, salary reduction, demotion, and/or dismissal from state service.*
- Criminal prosecution.
- Civil lawsuit.
- Termination of contract.

I, _____ expressly consent to the monitoring of my access to computer-based confidential information by CalVCB or an individual designated by CalVCB.

Certification

I have read, understand, and agree to abide by the provisions of the Confidentiality Statement and the CalVCB Information Security Policy, Memo number 06-00-003

I also understand that improper use of CalVCB files, data, information, and systems could constitute a breach of contract. I further understand that I must maintain the confidentiality of all CalVCB files, data, and information once my employment, contract, or affiliation with CalVCB ends. This signed Certification will be retained in my Official Personnel File in Human Resources.

If I am a contractor, I understand that it is my responsibility to share these contract provisions with any staff under my supervision and ensure that they comply with its provisions.

Signature	Date

Name (Print)

ATTACHMENT 7

Information Systems Security and Confidentiality Acknowledgement

I have read and understand the *CalVCB Information Systems Security and Confidentiality* requirements listed below. If an issue arises regarding these requirements during my daily work, I understand that I should refer to the *Acceptable Use of CalVCB Technology Resources Policy*, *Information Security Policy*, or contact my manager/supervisor to seek further clarification. I understand that failure on my part to comply with these requirements may result in punitive and/or disciplinary action up to, and including, termination.

I understand that I must:

- Read and understand the CalVCB Information Security Policy.
- Use CalVCB information assets and computer resources only for CalVCB business-related purposes.
- Ensure that my personal use of the internet is minimal and incidental use shall not violate other terms of established policy, be used in an unethical manner, or incur additional costs to the State.
- Access CalVCB systems and networks using only my assigned confidential user identifiers and passwords.
- Notify the CalVCB Information Security Officer immediately of any actual or attempted security violations including unauthorized access, theft, and destruction; misuse of systems equipment, software, or data.
- Take precautions to prevent virus contamination of CalVCB data files, and report any suspected virus or other destructive programs immediately to the Information Technology Section Help Desk.
- Exercise care in protecting confidential data including the use of encryption technology whenever it is required and/or provided by the CalVCB.
- Not attempt to monitor or tamper with another user's electronic communications or read, copy, change, or delete another user's files or software without the explicit agreement of the owner or per management direction.
- Change passwords at the prescribed expiration intervals.
- Not perform any act that interferes with the normal operation of computers, terminals, peripherals, or networks at CalVCB.
- Comply with all applicable copyright laws.
- Not disable the virus protection software installed on the CalVCB network and personal computers.

- Not attempt to circumvent data protection schemes and report to the Information Security Officer immediately any newly identified security vulnerabilities or loopholes.
- Follow certified destruction procedures for information disposal to prevent the unauthorized disclosure of data.
- Use only CalVCB approved hardware and software and never download from the internet or upload from home.
- Not use CalVCB electronic systems to send, receive, or store material that violates existing laws or is of a discriminating, harassing, derogatory, defamatory, threatening, or obscene nature.
- Not illegally use or copy CalVCB software.
- Use care to secure physical information system equipment from unauthorized access, theft, or misuse.
- Access only system areas, functions, or files that I am authorized to use.
- Not share individual account passwords.

I understand that CalVCB reserves the right to review electronic files, electronic messages, internet data and usage at its facility, and those files and messages stored on CalVCB systems may be disclosed under the California Public Records Act, discovered in legal proceedings, and used in disciplinary actions.

User Name (Print)	Division or Unit	
User Signature	Date	Phone Number
Manager/Supervisor Signature	Date	Phone Number

Filing Instructions

Staff/Contractor: Once completed, forward the form with original signature to your supervisor/manager.

Supervisor/Manager: Forwards the original to Human Resources to be filed in the staff's Official Personnel File.

Fraud Policy

Memo Number: 17-004
Issued July 10, 2017
Supersedes: 13-001
Effective immediately
Does not expire
Issued By: Legal Division

Purpose

To describe steps to be taken in the event fraud is suspected.

Policy

The California Victim Compensation Board (CalVCB) is committed to protecting the Restitution Fund against the risk of loss and will promptly investigate any suspected fraud, involving claimants, providers of service, representatives, and/or any other parties that have a business relationship with CalVCB. CalVCB will pursue every reasonable effort to obtain recovery of the losses from the offender or other appropriate sources.

This policy is not intended to address employee work performance, therefore, an employee's moral, ethical, or behavioral conduct should be resolved by the employee's supervisor/manager and the Human Resources Branch. If the suspected fraud involves another employee, the employee should contact his/her supervisor/manager immediately. If the suspected fraud involves the employee's supervisor/manager, the employee should contact the Human Resources Branch immediately.

Definition

Fraud is defined as a deception deliberately practiced in order to secure an unfair or unlawful gain. Actions constituting fraud include, but are not limited to:

- Any dishonest or fraudulent act.
- Any violation of federal, state, or local laws related to fraud.
- Forgery, unauthorized alteration, destruction, or manipulation of computer-related data or documents.
- Profiteering as a result of insider knowledge of CalVCB activities.

How to Report Fraud

Any employee who suspects fraud or has received an external fraud complaint shall immediately report it to his or her supervisor/manager and should not attempt to conduct the investigation personally. Managers

must complete an Investigation Referral Form (available on Boardnet), and submit it to the Deputy Executive Officer of their division for referral to the Provider Evaluation Team (PET).

If an employee receives a complaint of fraud from an external complainant, the employee should not attempt an investigation. The employee should gather contact information from the complainant and refer the matter to their supervisor for immediate submission to PET.

There are four reporting options available for external complainants:

1. Send an email to the fraud hotline at FraudHotline@victims.ca.gov
2. Call the toll-free fraud hotline at 1 (855) 315-6083
3. Write to the Legal Division at P.O. Box 350, Sacramento, CA 95812
4. Fax the complaint to (916) 491-6441

All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the PET Team.

Investigations

The PET has the primary responsibility for the investigation of all suspected fraudulent acts as defined in this policy. Pertinent investigative findings will be reported to executive management. Decisions to refer the results to the appropriate law enforcement and/or regulatory agencies for further investigation and/or prosecution will be made in consultation with executive management.

Any investigative activity required will be conducted objectively regardless of the suspected individual's position, title, length of service or relationship to CalVCB.

All information received in the course of a fraud investigation is treated as confidential to the extent permitted by law. CalVCB management will be alert and responsive to any reprisal, retaliation, threat, or similar activity against an employee because that employee has in good faith reported a suspected fraudulent activity. CalVCB employees must report any alleged reprisal, retaliation, threat or similar activity immediately.

In order to maintain the integrity of the investigation, CalVCB will not disclose or discuss the investigation results with anyone other than those who have a legitimate need to know. This is also important in order to avoid damaging the reputations of person(s) suspected but subsequently found innocent of wrongful conduct, and to protect CalVCB from potential liability.

Contacts

For questions, contact the Deputy Executive Officer for your division.

Password Policy

Memo Number: 17-012
Date Issued: March 24, 2017
Supersedes: 07-00-013
Effective Date: Immediately
Expires: Indefinite
Issued By: Information Technology Division

Policy

Any passwords used for User shall be complex and protected from unauthorized disclosure.

Purpose

To provide information regarding the minimum level of password protection required for CalVCB information assets.

Requirements

Passwords shall always be kept confidential.

Passwords shall not be viewable on a display device.

Password Standards

Passwords shall not contain personal information associated with the user that could be easily guessed.

Passwords shall not be words contained in English or foreign language dictionaries, spelling lists, or other lists of words. Passwords shall not be familiar acronyms, or slang expressions in common use.

Passwords shall not be the same as the User Identification (user id).

Passwords shall not consist solely of a repeating or sequential set of characters or numbers (i.e. 11111111, 12345678, ABCDEF, etc.)

Passwords shall contain characters from each character type indicated in the Password Character Type table that is appropriate to the level of security required for a specific role.

Changing Passwords

A password shall be changed immediately if it is suspected or discovered to be known by another individual.

Passwords shall be changed regularly. Refer to the Password Standards table for the maximum time allowed before a password must be changed.

All new passwords shall be significantly different from previous passwords (i.e. 1FONSE & 2FONSE are not significantly different).

Passwords protecting group accounts shall be changed immediately when a member of the group no longer needs access to the group account.

Initial Passwords

The distribution of initial user passwords shall use methods that ensure only the intended user learns the passwords.

Initial User Passwords shall conform to password practice requirements and standards.

Initial User Passwords shall be unique to each user.

The Initial User Password shall be changed by the user the first time it is used.

Session Inactivity Protection

After a user's login session has been inactive for the period of time specified in the Password Standards table, they must either re-enter their password or login again before the login session can be resumed.

Lockout

A User shall be locked out of the system when the standard threshold of unsuccessful attempts has been reached. Refer to the Password Standards table for those values.

Users that are locked out of the system as a result of too many unsuccessful attempts to enter a password must have their identity verified before they will be permitted access to that system.

Stored or Transmitted Passwords

Passwords that are stored on a system or transmitted across external networks shall be encrypted using a method that meets current 3-level Data Encryption Standards or hashed

using a message-digest algorithm is 3DES (or equivalent) or hashed using a method that is MD5 (or equivalent).

Business Partners Passwords

Access to business services provided by the CalVCB Internet sites by Employers and Business Partners shall be protected with a Business Partners Password.

User Passwords

User Passwords shall be used to authenticate a user's access to the CalVCB internal systems, applications, or resources.

Remote Access Passwords

Remote Access Passwords shall be used to authenticate a user's access to CalVCB internal systems and/or applications via Internet or inbound dial methods. Remote Access Passwords shall be randomly generated and valid for only one use.

Administration Passwords

Administration Passwords shall be used by administrators to authenticate themselves for access to restricted information and resources (i.e. administrator accounts or configuration files for critical system components).

Stored and Embedded Passwords

Systems and/or applications that must authenticate to each other shall use stored or embedded passwords.

Access to Stored and Embedded Passwords shall be restricted to the minimum number of staff necessary to support the systems and/or the applications that use them.

Stored passwords shall be contained in a file or database that is external to the application and can only be accessed by authorized systems, applications, and users.

Embedded passwords shall be contained within the system or application.

Default Passwords

Before any hardware and/or software are put into production at the CalVCB, any default passwords that it uses shall be set to values that conform to the Password Policy.

Exception Approval

Any non-compliance with the Password Policy shall be approved by the Chief Information Officer and Information Security Officer and should be documented.

Password Standards

Role	Business Partners	User	Remote Access	CaRES User	Admin (Service Accounts)	Stored	Embedded
Minimum password length (characters)	8	8	6 (Hardware Token)	8 and max of 32	8	8	8
Maximum time between password changes (days)	None	90	60 sec	90	90	None	None
Minimum time between password changes (days)	None	1	60 sec	none	1	None	None
Threshold of unsuccessful login attempts before account is disabled	3	5	3	5	3	5	3
Passwords must contain characters from each specified type of the Password Character Type Table	Based on Business partner password policy	1, 2	2	1,2,3	1,2,3,	1,2,3	1,2,3
Inactivity duration for session protection (maximum minutes)	20	20	20	20	20	None	None

Password Character Type Table

Types	Description	Example
Type 1	Letters (upper and lower case)	A, B, C, … Z a, b, c, … z
Type 2	Numerals	0, 1, 2, … 9
Type 3	Special characters (category 1)	Symbols in the top row of the keyboard: `~!@#$%^&*()-_=+

Guidelines

Automatic System Enforcement

Systems and/or applications should automatically enforce the password requirements and standards when automatic enforcement is possible.

Encrypted Transmission

Passwords should be encrypted when transmitted across internal networks.

Writing Down Passwords

Users should memorize their passwords and not write them down. If a password must be written down, the following precautions should be observed:

- Do not write down your password while you are in a public area where others could observe your writing.
- Do not identify your password as being a password.
- Do not include the name of the account and the dial-in telephone number of the system on the same piece of paper.
- Mix in extra characters or scramble the written version of the password in a way that you will remember, making the written version different from the real password.
- Do not attach the password to your terminal, keyboard, or any part of your computer or office furniture.
- Store a written password in a secure place like a wallet or purse.

Minimizing the Number of User Passwords

Systems shall be developed in a manner so the number of different passwords a user must know is minimized.

Change Embedded Password

Embedded passwords shall be changed when the programs they affect are also changed for routine enhancements or maintenance.

Accounts associated with stored or embedded passwords shall have account names that are difficult to guess to lessen the likelihood that these accounts can be disabled by unauthorized logon attempts as outlined in the Passwords Standards table.

Account Names for Stored and Embedded Passwords

Passwords shall be changed when a system/application is put into production so that the production passwords are known only to the Production Control staff and the system/application/data owner.

Compliance and Authority

Refer to the CalVCB Information Security Policy.

Who to contact for questions

For any questions about this Memo please contact your supervisor or manager, or the CalVCB Information Security Officer by e-mail at InfoSecurityandPrivacy@victims.ca.gov.

ATTACHMENT 10

Privacy Policy

Memo Number: 17-010
Date Issued: 1/1/17
Supersedes: 16-007
Effective Date: Immediately
Expires: Indefinite
Issued By: Information Technology Division

Purpose

The purpose of this Policy is to protect employees and the California Victim Compensation Board (CalVCB) from actions that would:

- Damage the reputation of the CalVCB.
- Endanger employees, contractors, or citizens that rely on CalVCB.
- Present a legal risk to CalVCB.

Policy

It is the Policy of CalVCB that:

- All personal, and personally identifiable information (PII) collected by CalVCB is necessary for the organization to perform its function.
- CalVCB will not retain PII for any longer than necessary to comply with the law, policy, regulations, and/or to perform its function.
- Staff will be trained on appropriate methods, classification of, and purposes for collecting PII.
- PII will be disposed of by confidential destruct.
- Users who violate the Policy will be subject to disciplinary action up to, and including, dismissal. Further, CalVCB will report suspected breaches of privacy to law enforcement, and the CA Information Security Office.
- Staff has the right to access their information that is gathered, stored, or used by CalVCB. Staff may request and view their information according to the Information Practices Act and State Policy.

Definition

- Privacy is defined as the freedom from secret surveillance, or unauthorized disclosure of one's personal data or information, as by a government, corporation, or individual.
- Privacy is the right of people to be free from unwarranted viewing, recording, photographing, and invasion into one's personal life. Ordinary citizens have a qualified right to privacy.

Applicability

- This Policy applies to all employees, temporary staff, contractors, consultants, and anyone performing work on behalf of CalVCB.
- If any provisions of this Policy are in conflict with a Memorandum of Understanding (MOU) with a State employee union, the applicable sections of the MOU will be controlling.

Management Responsibility

- Establish a Privacy Officer who will be responsible for maintaining the privacy program at CalVCB.
- Authorize staff to collect appropriate forms of personal and personally identifiable information.
- Ensure that staff has appropriate training.
- Ensure that staff has reviewed all appropriate policies.
- Ensure that staff has signed the Privacy Policy Acknowledgement Form upon appointment and annually thereafter.
- Report abuse or suspected privacy violations immediately to the Information Security & Privacy Officer.

Staff Responsibility

- Read the Privacy Policy and sign the acknowledgment form upon appointment and annually thereafter.
- Follow all privacy procedures and processes.
- Immediately report any privacy violation to their supervisor and/or Information Security & Privacy Officer.
- Secure all PII so no unauthorized person can obtain access.

- Properly dispose of PII.

Privacy Officer Responsibility

- To manage the privacy program.
- To ensure that privacy training is taken by all staff annually.
- To respond to privacy breaches in a timely manner and report to appropriate authorities.
- To maintain a robust privacy program that protects the privacy of staff and participants.
- The Information Security Officer will have the dual role as the CalVCB Privacy Officer.

Acceptable Use

Official CalVCB business needs only.

Monitoring

Managers will monitor staff to ensure that no PII is left exposed.

Incident Reporting

All incidents must be reported immediately to a manager/supervisor and the Information Security & Privacy Officer.

Violations

All employees who violate this Policy may be subject to disciplinary action up to, and including, dismissal.

Compliance

- All employees must read and sign a Privacy Policy Acknowledgement Form before being allowed to handle PII.
- The form will be retained in the staff's Official Personnel File.

Authority

- Government Code sections 11019.9, 13952 to 13954

- Information Practices Act of 1977 (Civil Code section 1798 et seq.)
- SAM 5310
- SIMM 5310

Other Applicable CalVCB Policies

- Acceptable Use of CalVCB Technology Resources Policy
- Information Security Policy
- Telework Policy
- Mobile Device Policy

Contact

For any questions about this Policy, please contact your immediate manager/supervisor or Information Security & Privacy Officer at InfoSecurityandPrivacy@victims.ca.gov

Distribution

All CalVCB staff

Acceptable Use of Technology Resources

Memo Number: 17-005
Date Issued: 1/11/17
Supersedes: 15-003
Effective Date: Immediately
Expires: Indefinite
Issued By: Information Technology Division

Purpose

The Victim Compensation Board's (CalVCB) *Acceptable Use of Technology Resources Policy* does the following:

- Defines the rules for the use of the CalVCB network, wireless network, computer systems, Internet, and other technology resources such as email, desktop workstations, mobile devices, and telephones.
- States clearly that state technology resources are to be used for state business purposes; and,
- Establishes that the Information Technology Division (ITD) routinely monitors CalVCB technology resources to identify improper use.

Policy

It is the policy of the CalVCB that:

- Use of technology resources must comply with the laws and policies of the United States Government and the State of California.
- Each user's assigned job duties and responsibilities are appropriate and regulated.
- Restrictions to CalVCB ITD assets are based on a staff person's business need (need-to-know).
- CalVCB's ITD staff may monitor the network continuously and/or periodically to ensure compliance.

Applicability

This Policy applies to:

- All employees, temporary staff, contractors, consultants, and anyone performing work on behalf of the CalVCB.

Note: If any provisions of this Policy are in conflict with a Memoranda of Understanding (MOU), the applicable sections of the MOU will be controlling.

Management Responsibilities

- Authorize staff to use the network-based resources for appropriate business need.
- Ensure that staff has reviewed all appropriate policies, and signed the Acceptable Use of Technology Resources Policy Acknowledgement form.
- Report any violations to the CalVCB Information Security Officer (ISO).

User Responsibilities

- Act in the best interest of the CalVCB by adhering to this Policy.
- Use discretion when using CalVCB information technology assets.
- Access only the CalVCB resources that they are authorized to use.
- Use the system only for its designed purposes.
- Keep all passwords confidential.
- Refrain from illegal activities, including unethical or obscene online behavior.
- Access only acceptable material on the Internet.
- Report any violations to a supervisor/manager and ISO.

Requests for Exception

Requests for exceptions must be submitted to the CalVCB Help Desk via email at Helpdesk@victims.ca.gov or call x3800 during business hours from 8:00 AM to 5:00 PM.

Acceptable Activities

The following are examples of acceptable activities:

- Access only those systems and information assets required to perform current CalVCB duties.

- Using a CalVCB state-issued IT asset to connect to CalVCB services to conduct CalVCB business activities.
- Accessing folders, files, and images stored on the CalVCB network for business purposes that are consistent with the staff person's job duties and network privileges.
- Using approved training material related to a user's duties for business-related knowledge or professional growth.
- Use the Internet to view sites, such as governmental and professional societies.
- Incidental use of Internet during breaks and lunch. (Incidental use must be minimal and must comply with all applicable CalVCB policies, practices, and guidelines).

Restriction on the Use of State IT Resources

The following are examples of unacceptable activities:

- Per Government Code section 8314, the following restrictions apply: incidental personal use that may create legal action, embarrassment, or interferes with the employee's normal work.
- Use of CalVCB IT resources for personal business, or personal gain.
- Intentionally attempting to access information resources without authorization.
- Accessing another employee's IT resource without permission.
- Using another employee's log-on identification credentials.
- Use for any illegal, discriminatory, or defamatory purpose, including the transmission of threatening, obscene, or harassing messages.
- Interfering with another employee's ability to perform their job duties or responsibilities.
- Browsing inappropriate websites such as those that contain nudity or sexual content, malicious content, or gambling.
- Installing or connecting unauthorized software or hardware on a CalVCB-owned and/or managed information resource.
- Storing personal nonbusiness-related data, such as pictures and multi-media files, on any CalVCB IT resource.
- Transmitting confidential information to external recipients without using encryption approved by the CalVCB ISO, and being necessary to execute the employee's specified job duties and responsibilities.

Incident Reporting

Any incident must be reported immediately to a supervisor/manager and the ISO.

Violations

Employees who violate this Policy may be subject to revocation of their access to the network, and disciplinary action up to, and including, dismissal.

The CalVCB will investigate all alleged violations and take appropriate action.

Compliance

All employees must read the CalVCB *Acceptable Use of Technology Resources Policy, and* sign an acknowledgement form upon appointment, and annually thereafter.

Authority

- Government Code sections 19572 and 19990.
- State Administrative Manual (SAM) sections 5300 through 5365.3
- Government Code Section 8314
- Applicable employee Memoranda of Understanding
- State Information Management Manual (SIMM)

Other Applicable CalVCB Policies

All employees, temporary staff, contractors, vendors, and consultants who access the CalVCB network for business purposes must comply with all State and CalVCB policies and procedures, including, but not limited to:

- Information Security Policy
- Password Policy
- Mobile Device Policy
- Telework Policy
- Privacy Policy
- Mobile Device Policy
- Wireless Access Policy

Contact

For any questions about this Policy, please contact your immediate supervisor/manager or the CalVCB ISO.

ATTACHMENT 12
California Victim Compensation Board
Acknowledgement of Polices

1. **Information Security Policy (Attachment 5)**

   I have read, understand, and agree to abide by the provisions of the Information Security Policy.

2. **Information Systems Security and Confidentiality Policy (Attachment 7)**

   I have read, understand, and agree to abide by the provisions of the Information Systems Security and Confidentiality Policy.

3. **Fraud Policy (Attachment 8)**

   I have read, understand, and agree to abide by the provisions of the Fraud Policy. I understand that if an issue arises regarding these requirements during my daily work and I suspect dishonest or fraudulent activity, I should immediately notify my Joint Powers (JP) or Criminal Restitution Compact (CRC) supervisor/manager and/or the CalVCB's Performance Standards, Audits and Quality Assurance Office (PAQ) for review. When the employee believes his or her supervisor/ manager is involved in the fraudulent activity, the employee should contact the PAQ directly.

   In referring the matter, the JP or CRC employee must complete an Investigation Referral Form and forward to PAQ.

   I also understand that failure on my part to comply with these requirements may result in punitive and/or disciplinary action up to, and including, termination of the JP or CRC contract.

   I also understand that failure on my part to comply with these requirements may result in punitive and/or disciplinary action up to, and including, termination of the contract.

4. **Password Policy (Attachment 9)**

   I have read, understand, and agree to abide by the provisions of the Password Policy.

5. **Privacy Policy (Attachment 10)**

   I have read, understand, and agree to abide by the provisions of the Privacy Policy.

6. Acceptable Use of Technology Resources (Attachment 11)

I have read, understand, and agree to abide by the provisions of the Acceptable Use of Technology Resources policy.

7. Incompatible Activities (Exhibit D, section 4)

I have read, understand, and agree to abide by the provisions of the Exhibit D, section 4, Incompatible Activities. I understand that I shall not engage in any work activity that is clearly inconsistent, incompatible, in conflict with, or adverse to my duties. I also understand that if I am unwilling or unable to abide by the provisions, I shall no longer be assigned to perform the services required by the Agreement.

County Employee's Signature	**Date**
Typed or Printed Name	**Classification Title**
Manager/Supervisor Signature	**Date**
Type or Printed Name	**Classification Title**
County	**Contract Number**