

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

**STANDARD AGREEMENT**

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER <b>S24-012</b>	PURCHASING AUTHORITY NUMBER (If Applicable) <b>VCB-7870</b>
------------------------------------	--

1. This Agreement is entered into between the Contracting Agency and the Contractor named below:

CONTRACTING AGENCY NAME  
California Victim Compensation Board

CONTRACTOR NAME  
San Francisco District Attorney's Office

2. The term of this Agreement is:

START DATE  
July 1, 2024

THROUGH END DATE  
June 30, 2027

3. The maximum amount of this Agreement is:  
\$2,530,992.00 (Two million five hundred thirty thousand nine hundred and ninety two dollars and zero cents)

4. The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of the Agreement.

Exhibits	Title	Pages
Exhibit A	Scope of Work	5
Exhibit B	Budget Detail and Payment Provisions	5
Exhibit B-1	Budget Worksheet	2
Exhibit C *	General Terms and Conditions	GTC 04/2017
Exhibit D	Special Terms and Conditions	15
Attachment 1	Training Request Form	1
Attachment 2	County Purchase Request Form	3
Attachment 3	CaIVCB Asset Identification Form	2
Attachment 4	County Inventory Form	1
Attachment 5	Information Security Policy	6
Attachment 6	Confidentiality Statement	3
Attachment 7	Information Systems Security and Confidentiality Acknowledgement	2
Attachment 8	Fraud Policy	3
Attachment 9	Password Policy	6
Attachment 10	Privacy Policy	4
Attachment 11	Acceptable Use of Technology Resources	5
Attachment 12	Acknowledgement of Policies	1
Attachment 13	Production Expectations and Performance Criteria	1

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES  
**STANDARD AGREEMENT**  
 STD 213 (Rev. 04/2020)

AGREEMENT NUMBER <b>S24-012</b>	PURCHASING AUTHORITY NUMBER (If Applicable) <b>VCB-7870</b>
------------------------------------	--

Exhibits	Title	Pages
Attachment 14	Board Resolution	

Items shown with an asterisk (\*), are hereby incorporated by reference and made part of this agreement as if attached hereto.  
 These documents can be viewed at <https://www.dgs.ca.gov/OLS/Resources>

IN WITNESS WHEREOF, THIS AGREEMENT HAS BEEN EXECUTED BY THE PARTIES HERETO.

**CONTRACTOR**

CONTRACTOR NAME (if other than an individual, state whether a corporation, partnership, etc.)  
 San Francisco District Attorney's Office

CONTRACTOR BUSINESS ADDRESS 350 Rhode Island Street, North Building, Suite 400N	CITY San Francisco	STATE CA	ZIP 94103
--	-----------------------	-------------	--------------

PRINTED NAME OF PERSON SIGNING Brooke Jenkins	TITLE District Attorney
--	----------------------------

CONTRACTOR AUTHORIZED SIGNATURE <b>Brooke Jenkins</b> <small>Digitally signed by Brooke Jenkins Date: 2024.03.15 10:45:57 -07'00'</small>	DATE SIGNED 3/15/24
---	------------------------

**STATE OF CALIFORNIA**

CONTRACTING AGENCY NAME  
 California Victim Compensation Board

CONTRACTING AGENCY ADDRESS 400 R Street, Suite 400	CITY Sacramento	STATE CA	ZIP 95811
---	--------------------	-------------	--------------

PRINTED NAME OF PERSON SIGNING Lynda Gledhill	TITLE Executive Officer
--	----------------------------

CONTRACTING AGENCY AUTHORIZED SIGNATURE	DATE SIGNED
---	-------------

CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	EXEMPTION (If Applicable)
--	---------------------------

**EXHIBIT A  
SCOPE OF WORK**

1. This Agreement is entered between the San Francisco District Attorney's Office (Contractor) and the California Victim Compensation Board (CalVCB), collectively known as the "parties".
2. The purpose of this Agreement is to authorize funding of the Joint Powers to support contracted staff who assist in processing applications, bills, emergency awards, and provide ongoing customer service throughout the claims process to provide restorative financial assistance to victims of crime.
3. Services shall be provided during the term of July 1, 2024, or upon final approval from the California Department of General Services (DGS), whichever occurs later, through June 30, 2027. No work shall begin before that time and Contractor shall not receive payment for work performed prior to approval of the Agreement. The services shall be provided, Monday through Friday, excluding State and county holidays. The Contractor shall obtain approval from the Contract Manager or designee prior to any temporary changes in schedule, including overtime.
4. The services shall be performed throughout the State of California designated sites as agreed upon by CalVCB and Contractor.
5. The project representatives during the term of this Agreement will be:

<b>STATE AGENCY</b>	<b>CONTRACTOR</b>
California Victim Compensation Board	San Francisco District Attorney's Office
Name: Lynda Gledhill	Name: Brooke Jenkins
Phone: 916-491-3501	Phone: 628-652-4000
Fax: 916-491-6435	Fax: 628-652-4101
Email: <a href="mailto:Lynda.Gledhill@victims.ca.gov">Lynda.Gledhill@victims.ca.gov</a>	Email: Brooke.Jenkins@sfgov.org

For additional information, direct all inquiries to:

<b>STATE AGENCY</b>	<b>CONTRACTOR</b>
California Victim Compensation Board	San Francisco District Attorney's Office
Unit: Joint Powers Unit	Section/Unit: District Attorney/Victim Services Unit
Attention: Reginald Brown	Attention: Karima Baptiste
Address: 400 R Street, Suite 400 Sacramento, CA 95811	Address: 350 Rhode Island Street, North Building, Suite 400N, San Francisco, CA 94103

**EXHIBIT A  
SCOPE OF WORK**

Phone: 916-491-3809	Phone: 628-652-4114
Fax: N/A	Fax: 628-652-4101
Email: <a href="mailto:Reginald.Brown@victims.ca.gov">Reginald.Brown@victims.ca.gov</a>	Email: Karima.c.baptiste@sfgov.org

6. Either party may change any portion of the above contact information by providing thirty (30) days written notice of the change to the other party. No amendment of this agreement is needed to make such a change.
7. Contractor agrees to provide all labor, materials, and incidentals necessary to provide the services described in this Agreement.
8. The CalVCB and San Francisco District Attorney's Office agree:

A. Data Entry Verification and Review of Applications and Bills

Contractor shall enter data from applications and bills received from victims of crime for unreimbursed financial losses into CalVCB's automated claims management system. The Contractor shall accept and process applications from any applicant or individual submitting an application. Contractor shall verify and process claims and bills pursuant to the statutes, regulations, policies, and directives of CalVCB. The Contractor shall conduct data entry verification and review of applications and bills as assigned. The Contractor must accept and process all applications without discretion to decline any submission unless directed by CalVCB.

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 report any overpayments or suspected overpayments to [JPUnit@victims.ca.gov](mailto:JPUnit@victims.ca.gov) as soon as the overpayments are identified. If the Contractor has made a reasonable attempt to recover the overpayment but the overpayment was not recovered, then CalVCB will pursue collection of the overpayment from the overpaid party. For a detailed description of overpayment procedures refer to the CalVCB Manual.

**EXHIBIT A  
SCOPE OF WORK**

C. Emergency Expenses

Contractor shall determine eligibility for and administer emergency expenses consistent with subdivision (c) of Government Code section 13952.5 and pursuant to its separately authorized and 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 surrounding counties designated service area to the extent that such activities do not adversely affect the Contractor's ability to conduct data entry verification, review applications and bills, or its supervisory duties required under this Agreement.

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 any outreach or training. The Contractor shall utilize CalVCB resource materials for all outreach and training activities. At CalVCB's discretion, summary reports regarding outreach and training activities may be requested.

9. Services under this Agreement shall only be performed by staff that have satisfactorily completed all required training provided by CalVCB and certified by CalVCB as qualified to perform such duties.
10. The Contractor shall only use information collected under this Agreement for services identified in this Exhibit A, Scope of Work.
11. The Contractor shall use CalVCB's automated claims management system known as the Compensation and Restitution System (Cares2), 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 Cares2 system as stated in section 11, Exhibit D, Special Terms and Conditions.
12. The 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.

**EXHIBIT A  
SCOPE OF WORK**

13. 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 statute and as directed by the CalVCB. All processing staff shall have a minimum of five percent (5%) quality assurance established in the Cares2 system for each work item Application Intake, Eligibility Determination, Bill Intake, Bill Determination, and Income Loss Determination.
14. 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.
15. 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.

16. Hardware and Software Responsibilities

The Contractor shall provide all necessary hardware and software to complete services as stated in this Exhibit A, Scope of Work.

17. Incompatible Work Activities

Contractor's staff assigned to perform services for CalVCB under this Agreement shall not:

- A. 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 under the CalVCB program.
- B. Use information obtained while doing work under this Agreement for personal gain or the advantage of another person.
- C. Disclose any confidential information except as required by law or authorized by CalVCB. Confidential information includes, but is not limited to, information about applicants, applications and documents associated with applications.
- D. Provide or use the names of persons or records of the CalVCB for a mailing list

**EXHIBIT A  
SCOPE OF WORK**

which has not been authorized by CalVCB.

- E. Represent himself or herself as a CalVCB employee.
- F. Take any action with regard to a CalVCB claim or restitution matter with the intent to obtain private gain or advantage.
- G. Involve him or herself in the handling of any claim or restitution matter when he or she has a relationship (business or personal) with a claimant or other interested party.
- H. Knowingly initiate any contact with a claimant, person for whom restitution may be sought, or person against whom restitution may be collected, unless the contact is for the purposes of carrying out the services under this Agreement and is done in an appropriate manner.

In accordance with all applicable laws, all contracted staff are required to comply with the State's efforts to maintain a drug-free working environment. CalVCB has a vital interest in maintaining safe, healthy, and efficient working conditions. Contracted staff's ability to perform duties safely and effectively can be impaired by use of illegal drugs, alcohol, legally prescribed medications or a combined use of these substances. Substance abuse poses serious safety and health risks not only to contracted staff, but to fellow workers and others with whom the contracted staff has contact.

It shall be the Contractor's responsibility to ensure that every staff person assigned to provide contracted services to CalVCB is made aware of and abides by this provision. If an assigned staff person is unwilling or unable to abide by this provision, the staff person should no longer be assigned to perform the services required by the Agreement. Any questions should be directed to the Contract Manager.

- 18. If there is any conflict between Attachments 1 through 13, and any provisions in the STD 213 Agreement, including Exhibits A, B, C, and D, the provisions in the Agreement shall prevail over the Attachments.

**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 permitted by the terms of this Agreement, and as reflected in the Budget Worksheet (Exhibit B-1).
- B. The Contractor shall submit the invoice for reimbursement once a month. The monthly invoices shall be sent to CalVCB by the 30<sup>th</sup> day of the month following the month of service. The invoice shall include the Agreement Number S24-012 and be sent to:

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

Or by email to: [accountingmailbox@victims.ca.gov](mailto:accountingmailbox@victims.ca.gov)

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

- County Name
- Date of Invoice
- Invoice Number
- Date of Service
- Direct Costs
- Overhead Costs
- Employee Fringe Benefits
  - Eligible Fringe Benefits include, but are not limited to:
    - Standard Retirement
    - OASDI
    - Medicare
    - Health Insurance
    - Dental Insurance
    - Vision Insurance
    - Life Insurance
    - Other, as approved by CalVCB
  - Ineligible Benefits include, but are not limited to:
    - Allocated costs
    - Parking
    - Allowances, such as cell phones, vehicles, gas, etc.
    - Bonuses and monetary awards



**EXHIBIT B**  
**BUDGET DETAIL AND PAYMENT PROVISIONS**

- Flex Benefit Plan
  - Housing Fund or allowance
  - Savings Plan
  - Time sheets or attendance records with month/year for each employee
  - Position/classification, time base, and monthly/weekly/hourly rate for all staff
  - Other approved expenses with approved supporting documentation
- D. Items not listed are subject to approval and payment at CalVCB's discretion.
- E. Invoices must be based on the hours worked in a pay period, not on any other time period for which county staff are paid.
- F. CalVCB reserves the right to deny any monetary adjustments to the contract, during the contract term, including Cost-of-Living Adjustments issued by the county.
- G. Fringe benefits charged to this contract are subject to CalVCB approval and shall not exceed benefit rates applicable to State employees. Fringe benefits in excess of seventy-five percent (75%) will be subject to additional scrutiny.
- H. CalVCB may request backup documentation to support the amount billed. This includes but is not limited to: accounting reports, receipts, functional timesheets, employee pay stubs, Salary and Benefit Reports, etc.
- I. Failure to provide the required backup documentation may result in a processing delay and/or denial of payment.
- J. Final Invoice

The Contractor shall submit the June invoice within 30 calendar days after June 30<sup>th</sup> of each year. The final reimbursement to the Contractor shall be contingent upon the receipt and approval of the final year-end invoice received by CalVCB.

**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 further provisions of this Agreement.

**EXHIBIT B**  
**BUDGET DETAIL AND PAYMENT PROVISIONS**

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 cancel this Agreement with no liability to CalVCB or offer an agreement amendment 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 2024-2027 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 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 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, Government Code 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;

**EXHIBIT B  
BUDGET DETAIL AND PAYMENT PROVISIONS**

- 2) Yearly, 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. The Contractor shall submit to the Contract Manager a written request via email prior to procuring such goods or services. 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 price quotations shall be submitted or adequate justification provided for the absence of bidding. Unless expressly specified in the quotation, all quotations shall remain valid for a period not to exceed 30 days. The Contractor is responsible for submitting valid quotations.
- 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).

<b>Fiscal Year</b>	<b>Date</b>
FY 2024/2025	July 1, 2024
FY 2025/2026	July 1, 2025
FY 2026/2027	July 1, 2026

5. Record Keeping

**EXHIBIT B  
BUDGET DETAIL AND PAYMENT PROVISIONS**

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 \$2,530,992.00

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

Fiscal Year	Dollar Amount
FY 2024/2025	\$843,664.00
FY 2025/2026	\$843,664.00
FY 2026/2027	\$843,664.00

C. Subject to CalVCB's approval, the Contractor may modify the Budget Worksheet (Exhibit B-1) without formal amendment to the Agreement to reflect changes in the following categories: employee name(s), salary/hourly rate range, percentage of time spent on CalVCB matters, fringe benefits (including percentage of salary), and overhead costs (not to exceed 10% of salary and benefits) provided the total budget does not exceed \$843,664.00 for each fiscal year. The B-1 may be modified no more than three times per fiscal year, except when necessitated by changes to employee name(s).

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.



Name of County  
Contract Number

San Francisco  
S24-012

FY 2024-25

**OPERATING EXPENSES**

Contract Amount

Rent (Square feet=_____)	_____
Utilities	_____
Insurance	_____
Equipment rental	_____
Equipment repair	_____
Office supplies	_____
Telephone	_____
Postage	_____
Expendable equipment (non-capitalized assets)	_____
Overhead	_____
Training	_____
Data Processing	_____
Other	_____
Travel - Meetings, conferences	_____
Travel - Training	_____

**TOTAL OPERATING EXPENSES**

**\$ -**

**TOTAL AMOUNT OF CONTRACT FOR THIS YEAR**

**\$ 843,664**

Please indicate if county staff are paid bi-weekly or monthly: bi-weekly

Does your county direct any non-VCGCB funding toward the services provided under this contract?

Yes  No

If **yes**, please list any additional funds provided for operation of this verification unit.  
Please describe the source of funding.

	Source of funding	Amount
Personnel Services	General Fund (1.60 TE 8129 Claims Specialist - Imani Carter/Ferdinand Laxamana)	\$ 229,005
Operating Expenses	General Fund (Rent & Overhead)	\$ 287,504
Other		
	Total	<b>\$ 516,509</b>

**County Budget Officer Contact Information:**

Name: Eugene Clendinen, Chief Administration & Finance  
 Phone Number: 628-652-4030  
 Email Address: eugene.clendinen@sfgov.org

**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 Assistant Deputy Executive Officer (ADEO) of Administration, who may consider any written or verbal evidence submitted by the Contractor. The decision of the Administration ADEO, issued in writing, shall be CalVCB's final decision regarding the dispute.
- B. Neither the pendency of a dispute nor its consideration by the Administration ADEO 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. Termination for Convenience

CalVCB or the Contractor reserves the right to terminate this Agreement upon thirty (30) days written notice to the other party. Invoicing of the above mentioned costs shall be submitted to CalVCB within thirty (30) calendar days of the date of termination.

4. Amendments

This Agreement may be amended in writing by mutual written consent of both parties.

5. Subcontracting

All subcontracting must comply with the requirements of the State Contracting Manual Volume 1, Section 3.06. Nothing contained in this agreement or otherwise shall create any contractual relation between the State and any subcontractors, and no subcontract shall relieve the Contractor of its responsibilities and obligations herein. The Contractor agrees to be as fully responsible to the State 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



**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

Contractor. The State shall have no obligation to pay or to enforce the payment of any moneys to any subcontractor.

6. Executive Order N-6-22 Russia Sanctions

On March 4, 2022, Governor Gavin Newsom issued Executive Order N-6-22 (the EO) regarding Economic Sanctions against Russia and Russian entities and individuals. "Economic Sanctions" refers to sanctions imposed by the U.S. government in response to Russia's actions in Ukraine, as well as any sanctions imposed under state law. The EO directs state agencies to terminate contracts with, and to refrain from entering any new contracts with, individuals or entities that are determined to be a target of Economic Sanctions. Accordingly, should the State determine Contractor is a target of Economic Sanctions or is conducting prohibited transactions with sanctioned individuals or entities, that shall be grounds for termination of this Agreement. The State shall provide Contractor advance written notice of such termination, allowing Contractor at least 30 calendar days to provide a written response. Termination shall be at the sole discretion of the State.

7. Americans with Disabilities Act

Contractor agrees to ensure that deliverables developed and produced, pursuant to this Agreement shall comply with the accessibility requirements of Sections 7405 and 11135 of the California Government Code, Section 508 of the Rehabilitation Act of 1973 as amended (29 U.S.C. § 794d), regulations implementing the Rehabilitation Act of 1973 as set forth in Part 1194 of Title 36 of the Code of Federal Regulations, and the Americans with Disabilities Act of 1990 (42 U.S.C. §§ 12101, et seq.). In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. California Government Code Sections 7405 and 11135 codify Section 508 of the Rehabilitation Act of 1973 requiring accessibility of EIT.

8. Regulations and Guidelines

All parties agree to abide by all applicable federal and state laws and regulations and CalVCB guidelines, procedures, directives, and memos as they pertain to the performance of this Agreement. Contractor agrees to pay Contractor staff in accordance with federal and state labor laws.

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

9. Program Evaluation and Monitoring

- A. The Contractor shall make available to CalVCB, and its representatives, for purposes of inspection, audit, and review, any and all of its books, papers, documents, financial records and other records pertaining to the operation of this Agreement. The records shall be available for inspection and review during regular business hours throughout the term of this Agreement, and for a period of three (3) years after the expiration of the term of this agreement.

10. 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. CalVCB shall reimburse compensable time off including vacation, sick, and annual leave accrued while performing services associated with this contract as 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 must maintain a clear separation of duties for processing claimant eligibility and payments. If a single individual is responsible and such separation of duties cannot be ensured, payments shall be forwarded to CalVCB's JP liaison staff for review and approval prior to payment being issued.

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.

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

- 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 Manager 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 Manager 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 his/her 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 staff to perform services other than those described in Exhibit A, Scope of Work, the Contractor shall request written authorization at least ten (10) calendar days prior to the 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.

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

- H. Contractor agrees to pay Contractor staff in accordance with federal and state labor laws.
- I. Requirements as described in Exhibit D, section 10, Special Terms and Conditions, are to be sent to:

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

Email: [JPUunit@victims.ca.gov](mailto:JPUunit@victims.ca.gov)

11. 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 the performance of services under this Agreement and periodically report performance evaluations to the Contractor.
- B. CalVCB shall set production and accuracy expectations and goals for services to be performed as described in Exhibit A, Scope of Work, for leads and supervisors. CalVCB's production expectations for staff are outlined in Attachment 13, which includes the types and amount of work to be completed within given timeframes. In addition to meeting the production expectations, Contractor shall perform the work in a quality manner, which includes an average 10% error or less for all processing work evaluated by CalVCB periodically throughout the term of this Agreement, CalVCB shall provide written notice of production and accuracy performance measures to the Contractor. If the Contractor fails to achieve production and/or 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 staff from the Agreement.
- C. CalVCB reserves the right to implement a CAP and revoke Cares2 access for staff whose production and/or accuracy is consistently poor or below average based on the performance criteria identified by CalVCB in Attachment 13, 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 shall not be reimbursable by CalVCB.

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

Contractor may replace staff in accordance with section 6 of Exhibit B, Budget Detail and Payment Provisions.

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

**12. Confidentiality of Records**

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 as specifically authorized by CalVCB. For additional information please refer to the Information Security Policy (Attachment 5). The Contractor, their supervisor/manager, and staff shall not print any documents containing PII from Cares2 or keep records separate from those in Cares2.

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 Executive Officer, Chief Deputy Executive Officer, or Chief Counsel.

CalVCB's Custodian of Records at CalVCB Headquarters in Sacramento is to be immediately notified of any request made under the Public Records Act (Gov. Code, §§ 7920.000, et. seq.) or the Information Practices Act (Civ. Code, §§ 1798, et. seq.) for information received or generated in the performance of this Agreement. No record shall be disclosed pursuant to any such request unless authorized by CalVCB's Legal Division. Please contact (916) 491-3651 or [CPRA@victims.ca.gov](mailto:CPRA@victims.ca.gov) with any requests.

The Contractor shall be responsible for any unauthorized disclosure by Contractor staff performing duties described in this Agreement, regardless of whether or not the services of such staff are paid for by CalVCB, and shall indemnify, defend and hold harmless the State, its officers, agents and employees from any and all claims, losses,

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

damages, penalties, fines, and attorney fees resulting from the unauthorized disclosure of CalVCB records by such staff .

To e-mail requests and correspondence related to this section of the Agreement, send to:

California Victim Compensation Board  
Joint Powers Unit  
[JPUnit@victims.ca.gov](mailto:JPUnit@victims.ca.gov)

13. Retention of Records

A. Application Records

The Contractor shall retain all documents related to applications entered into the Cares2, the CalVCB automated claims management system, for one year from the date the document is received. After one year, the Contractor shall contact the Joint Powers Unit to make arrangements for the documents to be destroyed consistent with the CalVCB Records Retention schedule.

B. Administration and Fiscal Records

The Contractor shall retain any other records relating to the operation of this Agreement, including, but not limited to, payroll, timekeeping, accounting records and electronic records, for seven years from the date the record is created.

C. All electronically retained documents shall have the same legal effect as an original paper document.

D. The Contractor shall not destroy any files or records without prior written authorization from CalVCB.

14. Subpoena

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 subpoenas for all records from CalVCB must be personally served on CalVCB at the California Victim Compensation Board, Attn: Legal Division at 400 R Street, Ste. 500, Sacramento CA 95811. The Contractor may also contact the Legal Division at (916) 491-3651 for assistance or questions.

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

When documents are subpoenaed, the Contractor shall provide CalVCB with all requested documents in the most expedient manner to meet the time constraints of the subpoena, including the use of overnight express mail.

The Contractor is not the Custodian of Records and may not testify in court on behalf of CalVCB.

15. Compliance with CalVCB Policies

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)
- Fraud Policy (Attachment 8)
- Password Policy (Attachment 9)
- Privacy Policy (Attachment 10)
- Acceptable Use of Technology Resources (Attachment 11)

Staff performing services under this agreement shall fill out and submit signed copies of the Confidentiality Statement (Attachment 6), Information Systems Security and Confidentiality Acknowledgement (Attachment 7), and Acknowledgement of Policies (Attachment 12) statements must be submitted within ten (10) business days of the start date of new staff and annually by July 30<sup>th</sup> of each year to:

California Victim Compensation Board  
Joint Powers Unit  
[JPUnit@victims.ca.gov](mailto:JPUnit@victims.ca.gov)

16. Utilization of Computer System

The Contractor shall ensure all Contractors performing the duties described in this Agreement comply with CalVCB policies, guidelines, procedures, directives, and memos, pertaining to the use of Cares2, regardless of whether the services of such staff persons are paid for by CalVCB. CalVCB reserves the right to revoke access to Cares2 at any time and to amend this agreement to align with changing or updating requirements around procurement, usage, disposition, and security of State Information Technology (IT) assets, which may include, but are not limited to, computer systems, software, and equipment.

17. Security and Privacy Compliance

The Contracted staff assigned to perform services for CalVCB must adhere to the

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

following provisions.

Staff shall not:

- A. Attempt to access the Cares2 application from any location other than their assigned work location.
- B. Share individual login ID or password with anyone else.
- C. Enable their computer to remember a password to the Cares2 application.
- D. Walk away from their computer without locking the screen (Ctrl-Alt-Delete).
- E. Send any Personal Identifiable Information (PII) via email. Staff should use application numbers, bill numbers, and initials only (if necessary). Staff should use encrypted email if they must send emails containing PII.
- F. Leave documents with PII unattended on printers or fax machines, in cubicles, offices or conference rooms.
- G. Visit untrusted websites or open any attachments/links from untrusted email.
- H. Uninstall or disable anti-virus software and automatic updates.
- I. Install any unauthorized or unlicensed software.
- J. Plug a mobile phone, personal USB drive or other peripheral device into the network system or desktop computer.
- K. Disclose any PII information to unauthorized users.

Any virus attacks, security violations, or privacy breaches should be reported immediately to your county Information Security Officer (ISO) and your supervisor. You must also notify the Joint Powers Unit Manager and copy CalVCB's IT Help Desk and ISO by sending an email to:

[ServiceDesk@victims.ca.gov](mailto:ServiceDesk@victims.ca.gov) and  
[InfoSecurityOffice@victims.ca.gov](mailto:InfoSecurityOffice@victims.ca.gov)

The Contractor and all staff with access to CalVCB computer systems are required to complete Information Security and Privacy Training, including at a minimum training



**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

regarding Social Engineering and Phishing, Privacy and Password Protection, Browsing Safely, and Ransomware at least annually.

The Contractor and staff shall submit the self-certification demonstrating completion of the required training within thirty (30) days of the Agreement start date to the CalVCB Contract Manager and annually thereafter. All new Contractors with access to CalVCB computer systems must complete the training within thirty (30) days from the date of hire.

Any training costs incurred by the Contractor for compliance with this section will be the responsibility of the Contractor.

In case of non-compliance, CalVCB may suspend access to CalVCB computer systems (including but not limited to Cares2 and CalVCB online) until such time as compliance is achieved and proof of compliance is provided to CalVCB.

**18. 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 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. 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.

All training-related 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.

**19. 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.

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

- 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.
- 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 the purposes authorized 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).

**20. 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, 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.

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

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.

21. 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: <https://calhr.benefitsprograms.info/state-employee/work-engagement-resources/travel-reimbursements/>. No out-of-state travel is authorized under this Agreement.

22. 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

23. 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.

24. 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 25 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

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

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 [servicedesk@victims.ca.gov](mailto:servicedesk@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.

**25. 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 procurements 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

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

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 any equipment that contains 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. The Contractor shall prepare and submit to CalVCB by July 30<sup>th</sup> 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 Joint Powers Unit 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 written 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.

**26. 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

**EXHIBIT D**  
**SPECIAL TERMS AND CONDITIONS**

in CalVCB and no further agreement will be necessary to transfer ownership to CalVCB. The Contractor shall furnish CalVCB with all necessary copies of data needed to complete the review and approval process.

## 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** \$

## 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 Date  
Victim Compensation Division

Agreement Number  Fiscal Year

**COUNTY PURCHASE REQUEST FORM**

<p>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, <b>equipment purchases over \$2,500 must be justified by the requesting County and approved by CalVCB</b>. If the request is not approved by CalVCB, the purchase will not be authorized for reimbursement through the Agreement. <b>A separate form must be completed for each piece of equipment being requested.</b></p>			
<b>1. COUNTY CONTACT INFORMATION</b>			
County:		Contract Number:	Fiscal Year Funded:
Contact Name:		Address:	Phone Number:
Email:			
<b>2. EQUIPMENT REQUEST</b>			
<p>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.</p> <p><i>Note: Acquisition of an equipment maintenance plan is the responsibility of the County and may be reimbursed through the Agreement.</i></p>			
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)			
<b>3. PURCHASE JUSTIFICATION</b>			
<p>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.</p>			
<b>4. COUNTY AUTHORIZATION</b>			
<p>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.</p>			
County Coordinator/Supervisor Signature:			Date:
<b>5. PURCHASE APPROVAL</b>			
<p>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.</p>			

**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.**



# ATTACHMENT 2

## COUNTY PURCHASE REQUEST FORM

<b>For CalVCB Staff Use Only:</b>		
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.		
<b>JPU Analyst Comments:</b>   		
This request is: <input type="checkbox"/> Approved <input type="checkbox"/> 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.		
<b>BSU Approval / Comments</b> (include Approved Changes or Denial details in this section):   		
This request is: <input type="checkbox"/> Approved <input type="checkbox"/> Approved w/Changes <input type="checkbox"/> Denied	Approved by (BSU Analyst):	
BSU Manager's Signature (required)	Signature:	Date:

## ATTACHMENT 2

### 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 30<sup>th</sup> 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)

<b>Asset Type</b>	
<b>Location/Address</b>	
<b>Make/Model</b>	
<b>Serial Number</b>	

### 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.

<b>Asset Tag Number</b> To be provided by CalVCB	<div style="border: 1px dashed gray; width: 80%; margin: 0 auto; padding: 20px 0;"> <p style="font-size: 2em; color: gray; margin: 0;">ASSET TAG</p> </div>
---	---

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



# 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](mailto:InfoSecurityandPrivacy@victims.ca.gov).

## Distribution List

All CalVCB staff

# Confidentiality Statement

VCB-22-20012 (Rev. 03/2023)

## Purpose of Confidentiality Statement

It is the policy of the California 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’s Information Security Policy, Memo Number 17-008 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.

## CalVCB 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, Chief Deputy 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, Chief Deputy 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, Chief Deputy 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, or medical or employment history.
- 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.

# Confidentiality Statement

VCB-22-20012 (Rev. 03/2023)

- Never release a copy of a law enforcement report to any individual, including a CaIVCB applicant. Law enforcement reports include, but are not limited to, reports by police, California Highway Patrol, sheriff departments, Department of Justice (DOJ), Federal Bureau of Investigation, Child Protective Services, and the Department of Social Services.
- Never disclose a Felon Status Verification Request completed by DOJ to any individual outside of CaIVCB.
- Never disclose any other information that is considered proprietary, copyrighted, or otherwise protected by law or contract.
- Inform the CaIVCB Custodian of Records at CaIVCB Headquarters in Sacramento immediately of any request made under the Public Records Act (Gov. Code, § 7920.000, et seq.) or the Information Practices Act (Civ. Code, § 1798, et seq.). No record shall be disclosed pursuant to any such request unless authorized by CaIVCB's Legal Division. Contact (916) 491-3651 or [CPRA@victims.ca.gov](mailto:CPRA@victims.ca.gov) with any requests.
- Inform a server of a subpoena that the subpoena requesting records from CaIVCB must be personally served on CaIVCB at the California Victim Compensation Board at 400 R Street, Suite 500, Sacramento, CA, 95811. Contact the CaIVCB Legal Office at (916) 491-3651 or [custodianofrecords@victims.ca.gov](mailto:custodianofrecords@victims.ca.gov) regarding any subpoena received by CaIVCB.
- Immediately report any suspected security incidents, virus attacks, security violations, or privacy breaches to the CaIVCB Information Security Officer (ISO) and your supervisor.

I, \_\_\_\_\_ acknowledge that as a state employee or individual performing work pursuant to a contract with CaIVCB, I am required to know whether the information I have been granted access to is confidential and to comply with this statement and the CaIVCB's Information Security Policy, Memo Number 17-008. If I have any questions, I will contact CaIVCB'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 13954, 7923.755, and 19990, subdivision (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 CaIVCB or an individual designated by CaIVCB.



# Confidentiality Statement

VCB-22-20012 (Rev. 03/2023)

---

## Certification

I have read, understand, and agree to abide by the provisions of the Confidentiality Statement and CalVCB's Information Security Policy, Memo Number 17-008.

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.

If I am a State employee, 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. This signed Certification will be retained by the Contract Manager and Business Services Unit as part of the contract file.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Name (Print)

\_\_\_\_\_  
Contract Number (If applicable)



## 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

# 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



## Fraud Policy

Memo Number: 17-004

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](mailto: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.



**Fraud Policy**

Memo Number: 17-004

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](mailto:InfoSecurityandPrivacy@victims.ca.gov).



# 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 CaIVCB Policies

- Acceptable Use of CaIVCB 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](mailto:InfoSecurityandPrivacy@victims.ca.gov)

## Distribution

All CaIVCB 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 (CaIVCB) *Acceptable Use of Technology Resources Policy* does the following:

- Defines the rules for the use of the CaIVCB 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 CaIVCB technology resources to identify improper use.

## Policy

It is the policy of the CaIVCB 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 CaIVCB ITD assets are based on a staff person's business need (need-to-know).
- CaIVCB'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](mailto: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
- Wireless Access Policy



## Contact

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

STATE OF CALIFORNIA

# Acknowledgement of Policies

VCB-22-20013 (Rev. 02/2024)



By checking each box below, I hereby acknowledge I have read, understand, and agree to adhere to the listed policies.

ATTACHMENTS	
<input type="checkbox"/> Information Security Policy (Attachment 5)	<input type="checkbox"/> Password Policy (Attachment 9)
<input type="checkbox"/> Confidentiality Statement (Attachment 6)	<input type="checkbox"/> Privacy Policy (Attachment 10)
<input type="checkbox"/> Information System Security and Confidentiality Acknowledgment (Attachment 7)	<input type="checkbox"/> Acceptable Use of Technology Resources (Attachment 11)
<input type="checkbox"/> Fraud Policy (Attachment 8)	

  

INCOMPATIBLE WORK ACTIVITIES
<input type="checkbox"/> I have read, understand, and agree to abide by the provisions of Exhibit A, Section 17, Incompatible Work 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 contract.

\_\_\_\_\_  
County Employee Name

\_\_\_\_\_  
County Employee Title

\_\_\_\_\_  
County Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Manager/Supervisor Name

\_\_\_\_\_  
Manager/Supervisor Title

\_\_\_\_\_  
Manager/Supervisor Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
County Name

\_\_\_\_\_  
Contract Number



ATTACHMENT 14

PLACE HOLDER  
THE BOARD RESOLUTION WILL BE AVAILABLE AFTER THE COUNTY RETURNS  
THE SIGNED CONTRACT

STANDARD AGREEMENT NUMBER S24-012

APPROVED AS TO FORM:

David Chiu, City Attorney

By: Sarah Crowley  
Sarah Crowley  
Deputy City Attorney

4/24/2024