

STATE OF CALIFORNIA  
**STANDARD AGREEMENT**  
 STD 213 (Rev 06/03)

AGREEMENT NUMBER <b>VC-8059</b>
REGISTRATION NUMBER

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

STATE AGENCY'S NAME  
**CALIFORNIA VICTIM COMPENSATION BOARD**

CONTRACTOR'S NAME  
**COUNTY OF SANTA BARBARA DISTRICT ATTORNEY'S OFFICE**

2 The term of this Agreement is: **JULY 1, 2018** through **JUNE 30, 2021**


3. The maximum amount of this Agreement is: **\$713,892.00**  
 Seven hundred thirteen thousand, eight hundred ninety two dollars

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.

Exhibit A – Scope of Work	3 Pages
Exhibit B – Budget Detail and Payment Provisions	3 Pages
Exhibit B-1 – Budget Page	1 Page
Exhibit C* – General Terms and Conditions (GTC 04/2017)	1 Page
Exhibit D – Special Terms and Conditions	9 Pages
Attachment I – CalVCB Information Security Policy (Memo 17-008)	6 Pages
Attachment II – CalVCB Confidentiality Statement and Certification	4 Pages
Attachment III – CalVCB Fraud Policy (Memo 17-004)	3 Pages
Attachment IV – Training Request Form	2 Pages
Attachment V – CalVCB Acknowledgement of Policies	1 Page
Attachment VI – Password Policy (Memo 17-012)	6 Pages
Attachment VII – County Purchase Request Form and Instructions	3 Pages
Attachment VIII – CalVCB County Inventory Form	1 Page
Attachment IX – CalVCB Asset Identification Form	2 Pages
Attachment X – Information Systems Security and Confidentiality Acknowledgement	2 Pages
Attachment XI – Acceptable Use of Technology Resources (Memo 17-005)	5 Pages
Attachment XII – Privacy Policy (Memo 17-010)	4 Pages

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 <http://www.dqs.ca.gov/ols/Resources/StandardContractLanguage.aspx>

**IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.**

<b>CONTRACTOR</b>		California Department of General Services Use Only          <input type="checkbox"/> Exempt per:
CONTRACTOR'S NAME (if other than an individual, state whether a corporation, partnership, etc.)		
<b>COUNTY OF SANTA BARBARA DISTRICT ATTORNEY'S OFFICE</b>		
BY (Authorized Signature)	DATE SIGNED (Do not type)	
	<b>4/30/18</b>	
PRINTED NAME AND TITLE OF PERSON SIGNING		
<b>Joyce E. Dudley, District Attorney</b>		
ADDRESS		
<b>1112 SANTA BARBARA STREET, SANTA BARBARA, CA 93101</b>		
<b>STATE OF CALIFORNIA</b>		
AGENCY NAME		
<b>CALIFORNIA VICTIM COMPENSATION BOARD</b>		
BY (Authorized Signature)		
		
PRINTED NAME AND TITLE OF PERSON SIGNING		
<b>Julie Nauman, Executive Officer</b>		
ADDRESS		
<b>400 R STREET, SUITE 500, SACRAMENTO, CA 95811</b>		

**EXHIBIT A  
SCOPE OF WORK**

The Contractor agrees to provide to the California Victim Compensation Board (CalVCB) services as described herein:

1. The data entry, verification, and processing of claims for the unreimbursed financial losses of victims of crime.
2. The Contractor shall verify and process applications and bills pursuant to the statutes, regulations, policies and directives of CalVCB.
3. The Contractor shall only use information collected under this contract for the purpose of verifying and processing claims.
4. The data entry, verification and processing of all applications and bills shall be performed by persons who have completed all required training provided by CalVCB, and who have been certified by CalVCB as qualified to perform such duties.
5. If an overpayment is identified as a result of an error the Contractor made, the Contractor shall follow the processes, policies and directives of CalVCB.
6. The Contractor shall administer emergency expenses under Government Code section 13952.5, subdivision (c) pursuant to a separate Revolving Fund contract.
7. The Contractor shall conduct data entry verification and review for applications and bills related to crimes that occurred in the following counties: Santa Barbara
8. CalVCB may at its sole discretion, redirect workload (1) from CalVCB to a Contractor or (2) from one Contractor to another Contractor or (3) from a Contractor to CalVCB. The Contractor may, with approval from the Deputy Executive Officer of the Victim Compensation Division at CalVCB, or the Deputy Executive Officer's designee, establish Memorandums of Understanding (MOU) to conduct data entry, verification, and review for applications and bills received from other counties.
9. The Contractor will use CalVCB's automated claims management system, known as the Compensation and Restitution System (Cares2), to perform the work under this contract. The Contractor shall ensure that all contracted staff persons performing duties under this contract comply with CalVCB guidelines, procedures, directives, and memos pertaining to the use of the Cares2 system.
10. The Contractor shall follow the processes, policies and directives of CalVCB when monies owed to the Restitution Fund in the form of liens and overpayments is identified.

**EXHIBIT A  
SCOPE OF WORK**

- 11. The Contractor shall also provide any paper application, bill or other related documents in its possession to CalVCB or its agent(s) on demand.
- 12. The Contractor shall maintain the highest customer service standards, and shall ensure that applications and bills are processed accurately and efficiently, that applicants receive prompt responses to their inquiries, and are treated with sensitivity and respect. Should CalVCB communicate to the Contractor any compliance issues or concerns about the foregoing, the Contractor shall respond to CalVCB within a reasonable time as requested by CalVCB. The Contractor shall demonstrate and apply trauma-informed principles and practices when communicating verbally and in writing with recipients of services.
- 13. The services shall be performed at:

County of	Santa Barbara
Office	District Attorney
Address	1112 Santa Barbara Street
City, State, Zip	Santa Barbara, CA 93101

- 14. The services shall be provided during regular business hours, as defined in the State Administrative Manual section 0180 and Government Code section 11020, Monday through Friday, except government holidays. At the beginning of each fiscal year, the Contractor shall provide a list of scheduled holidays for the coming year. The Contractor shall obtain approval from the CLASS Manager or designee in advance for any temporary changes in schedule or operating hours.
- 15. The Contractor shall provide outreach and training activities for stakeholders and members of the public within the designated service area to the extent that such activities do not adversely affect the Contractor's ability to conduct data entry, verification, and review of applications and bills. When conducting outreach or training activities, the Contractor shall inform CalVCB and utilize CalVCB resource materials.
- 16. The Contractor shall use forms and processes as required by CalVCB. Forms, letters or other documentation created by the Contractor and intended for the public, shall be submitted to CalVCB for review and approval prior to use.
- 17. The project representatives during the term of this agreement will be:

State Agency:	California Victim Compensation Board	Contractor:	County of Santa Barbara District Attorney
Name:	Dionne C. Bell-Rucker,	Name:	Megan Rheinschild, VW Program Director

**EXHIBIT A  
SCOPE OF WORK**

County Liaison and Support Section Manager	
Phone: (916) 491-3512	Phone:
Fax: (916) 491-6435	Fax:

Direct all inquiries to:

State Agency: California Victim Compensation Board	Contractor:
Section/Unit: Business Services Branch	Section/Unit:
Attention: Ryan Metzger, Contract Analyst	Attention:
Address: 400 R Street, Suite 400 Sacramento, CA 95811	Address:
Phone: (916) 491-3877	Phone:
Fax: (916) 491-6413	Fax:

**EXHIBIT B  
BUDGET DETAIL AND PAYMENT PROVISIONS**

**1. INVOICING AND PAYMENT**

- a. For services satisfactorily rendered, and upon receipt and approval of the invoices, CalVCB agrees to compensate the Contractor for actual expenditures permitted by the terms of this contract, as reflected in Exhibit B1, Budget.
- Invoices shall include the county name, contract number, month/year and time sheets or attendance records, including the employee name, position/classification, and time base, fringe benefit amounts and other expenses. Invoices and timesheets/attendance records should be submitted no later than the 30<sup>th</sup> day of the month following the month in which the expenses were incurred. Invoices should be submitted to:

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

- The Contractor shall submit a final year-end closeout invoice within forty-five (45) calendar days after June 30, 2019 for fiscal year 2018/2019, after June 30, 2020 for fiscal year 2019/2020, and after June 30, 2021 for fiscal year 2020/2021. The final reimbursement to the Contractor shall be contingent upon the receipt and approval of this closeout invoice by CalVCB.

**2. BUDGET CONTINGENCY CLAUSE**

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

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

The Contractor shall be paid by CalVCB from the Restitution Fund. Any payments shall be contingent upon the availability of funds in the Restitution Fund. Any funds paid shall not be a charge upon any federal monies or state General Fund monies. Funds provided under this agreement are not to be used for other services to victims

**EXHIBIT B  
BUDGET DETAIL AND PAYMENT PROVISIONS**

and shall not be used to supplant those currently provided by county funds, or grants administered by the California Emergency Management Agency.

**3. PROMPT PAYMENT CLAUSE**

CaIVCB shall pay all properly submitted, undisputed invoices within forty-five (45) days of receipt, in accordance with Chapter 4.5 of the Government Code beginning with section 927.

**4. COST LIMITATION**

The total amount of this agreement shall not exceed \$237,964.00 for fiscal year 2018/2019, \$237,964.00 for fiscal year 2019/2020, and \$237,964.00 for fiscal year 2020/2021. Funding shall be contingent upon availability of funds and shall be at the sole discretion of CaIVCB. The funding of this contract may be changed by written amendment to the contract, upon approval of CaIVCB.

The Contractor shall submit a budget for Fiscal Year 2018/2019 with this contract. The Contractor shall submit a proposed budget for Fiscal Year 2019/2020, no later than April 1, 2019 and for Fiscal Year 2020/2021, no later than April 1, 2020. The CLASS Manager shall provide written approval of the proposed budget(s) and any subsequent modification(s).

**5. REDUCTION OF CONTRACT AMOUNT**

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



**BUDGET WORKSHEET**

(Rev. 2/15)

**EXHIBIT B-1**

Page 2

**Name of County**  
**Contract Number**

**Santa Barbara**  
**VCGC8059**

**FY 2018-2019**

**OPERATING EXPENSES**

Rent (Square feet= _____)	Contract Amount
Utilities	_____
Insurance	_____
Equipment rental	_____
Equipment repair	_____
Office supplies	_____
Telephone	\$ 1,432
Postage	_____
Expendable equipment (non-capitalized assets)	_____
Overhead	\$ 11,047
Training	_____
Data Processing	\$ 4,938
Other	_____
Travel - Meetings, conferences	_____
Travel - Training	_____

**TOTAL OPERATING EXPENSES** **\$ 17,417**

**TOTAL AMOUNT OF CONTRACT FOR THIS YEAR** **\$ 237,964**

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

Does your county direct any non-VGCB 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	_____	_____
Operating Expenses	_____	_____
Other	_____	_____
	Total	<b>\$ -</b>

**County Budget Officer Contact Information:**

Name: Shawna Jorgensen  
 Phone Number: (805) 568-2304  
 Email Address: sjorgensen@co.santa-barbara.ca.us



**EXHIBIT C  
GENERAL TERMS AND CONDITIONS**

PLEASE NOTE: The General Terms and Conditions will be included in the contract by reference to Internet site <http://www.dgs.ca.gov/ols/Resources/StandardContractLanguage.aspx>.

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

1. PERSONNEL SERVICES AND WORKLOAD

- a. The Contractor shall submit by mail, email, or fax to CalVCB, in accordance with state law, a signed Statement of Economic Interests (Form 700) for each staff member performing work under this contract who is responsible for recommending an initial eligibility or payment decision, and for each person in a supervisory position over such staff members. The Form 700 must be mailed, emailed or faxed within five (5) business days of hiring new staff and, thereafter, must be submitted on an annual basis. The Contractor shall submit Form 700 no later than 30 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.
- b. The Contractor shall obtain written authorization prior to filling vacant or new positions related to this contract, reassigning personnel to or from the workgroup funded by this contract, or changing the time base of existing positions even though funding was previously requested and made part of the budget. Approval of such requests will be based upon CalVCB's review of the Contractor's workload, performance, and availability of funds. Personnel assigned to this contract shall possess the appropriate knowledge, skills and abilities to successfully perform the work. Hiring, transfers, or promotions of key personnel, such as program Managers, Supervisors and Leads must be approved in writing by the CalVCB CLASS Manager.
- c. The Contractor shall notify CalVCB when a staff person assigned to perform the functions of this contract has been absent, or is expected to be absent, for any reason, longer than two weeks. When the staff person is on leave, including vacation, sick, and annual leave, CalVCB shall compensate the Contractor for that period of time only if the staff person accrued leave during the time the staff person was assigned to perform the functions described in this contract. Further, the Contractor agrees to provide, at CalVCB's request, documentation verifying leave accrued under the agreement.
- d. The Contractor shall ensure that staff persons assigned to functions under this contract do not participate in criminal investigations or prosecution. The Contractor shall ensure that the staff persons assigned to functions under this contract do not also collect restitution or serve as a restitution specialist or victim advocate, with the exception of the director of the county victim assistance program.
- e. 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 contract, unless prior written authorization is obtained from the Deputy Executive Officer of the Victim Compensation Division or the Deputy Executive Officer's designee. The

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

Contractor will also obtain prior written authorization from the Deputy Executive Officer of the Victim Compensation Division or the Deputy Executive Officer's designee before including the salaries of any other administrative staff who are not directly involved in functions under this contract or the supervision of staff fulfilling functions under this contract in the budget.

- f. In addition, the Contractor shall obtain prior written permission from the Deputy Executive Officer of the Victim Compensation Division or the Deputy Executive Officer's designee if staff persons assigned to functions under this contract will perform any other county function. Should the Contractor assign a staff person to perform functions other than those described in Exhibit A, the Contractor shall request written authorization ten (10) days prior to the staff person beginning other county functions. CalVCB shall not reimburse the Contractor for other duties performed outside the scope of the contract.
- g. For each staff member performing services under this contract, the Contractor shall provide the name, business address, telephone number and email; the job title and description of duties; the name of his or her supervisor; the names of any staff supervised; and any other information as required by CalVCB. The Contractor shall also provide contact information for individual county victim assistance centers and advocate staff in any centers in other counties which send applications directly to the Contractor. The Contractor shall update the information anytime a change is made.

To mail requests and correspondence related to this section of the contract, send to: County Liaison and Support Section, California Victim Compensation Board, P.O. Box 3036, Sacramento, CA 95812-3036.

**2. INCOMPATIBLE ACTIVITIES**

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

1. Participate in a criminal investigation or prosecution.
- b. Engage in any conduct that is clearly inconsistent, incompatible, or in conflict with his or her assigned duties under the contract, including but not limited to: providing services that could be compensated under CalVCB.
- c. Use information obtained while doing work under the contract for personal gain or the advantage of another person.
- d. Disclose any confidential information to anyone, including, but not limited to, victim advocates, community-based organizations, law enforcement, prosecutors and others, except as required by law or authorized by the CalVCB. Confidential

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

information includes, but is not limited to, information about applicants, applications, crime documentation and other documents associated with applications.

- e. Provide or use the names of persons or records of CalVCB for a mailing list, which has not been authorized by CalVCB.
- f. Represent himself or herself as a CalVCB employee.
- g. Take any action with regard to a victim compensation claim or restitution matter with the intent to obtain private gain or advantage.
- h. Involve himself or herself in the handling of any claim or restitution matter when he or she has a relationship (business or personal) with a claimant or other interested party.
- i. 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 the contract and is done in an appropriate manner.

All confidential information obtained during the performance of the contract duties shall be held in strict confidence.

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 these provisions. If an assigned staff person is unwilling or unable to abide by these provisions, the staff person shall no longer be assigned to perform the services required by the contract and that person's salary will not be paid by CalVCB.

**3. PERFORMANCE ASSESSMENT**

CalVCB shall assess and evaluate the Contractor's performance in a manner consistent with those assessments and evaluations currently in place for CalVCB's claims processing staff.

- 2. CalVCB shall monitor performance under the contract and periodically report performance to the Contractor.
- 3. CalVCB reserves the right to revoke access to CalVCB's database of any Contractor's staff whose performance is consistently poor or below average based on the performance criteria used by CalVCB or who does not comply with the contract provisions. Any Contractor's staff whose access has been revoked shall no longer be authorized to process claims and the staff person's position will no

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

longer be funded by CalVCB. The Contractor will provide replacement staff, contingent upon approval by CalVCB CLASS Manager or designee.

4. CalVCB shall set performance and production expectations or goals related to the fulfillment of the services in this contract. Those expectations may include, but are not limited to, time frames for completion of work, amount of work to be completed within given time frames, and standards for the quality of work to be performed. CalVCB will provide written notice of performance and production expectations to the Contractor. If the Contractor fails to achieve performance and production expectations set by CalVCB as set forth in the written notice, CalVCB reserves the right to reduce the amount of the contract or terminate the agreement upon 30 days' notice.
5. CalVCB shall require county supervisors to utilize production, aging and workload reports provided by CalVCB, to maintain the level of production as outlined by CalVCB. The Contractor shall inform the CLASS Manager or designee of performance or other staffing issues immediately upon identification.

**4. PROGRAM EVALUATION AND MONITORING**

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 contract. The records shall be available for inspection and review during regular business hours throughout the term of this contract, and for a period of three (3) years after the expiration of the term of this contract.

**5. JOB-REQUIRED TRAINING**

CalVCB may reimburse salaries, benefits and travel costs for the Contractor's staff to attend job-required training, meetings, hearings, conferences or workshops. All such costs are included within the maximum agreement amount as reflected in the attached budget.

The Contractor shall obtain prior written authorization from CalVCB to attend trainings, meetings, hearings, conferences or workshops that are not job-required. The request is to be submitted on the Training Request Form (Attachment IV to this contract) and must be forwarded to the CLASS Manager or designee for approval prior to the training date. Approval for reimbursement for the requested training is at the discretion of CalVCB.

**6. MOVING**

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

6. CalVCB shall not reimburse any costs associated with the relocation of the Contractor's staff performing under this contract.
7. The Contractor shall obtain written authorization from CalVCB to relocate computer terminals far in advance as possible before any planned move. The request should be emailed to the CLASS Manager or designee for approval.
8. Notification of relocation shall include the new address, including room number and the name, title, address, and phone number of a contact person who is responsible for telephone line and computer/electrical cable installation.
9. The Contractor's Information Technology Department must notify CalVCB's Information Technology Section and CLASS of any change of a public internet protocol (IP) address within one business day.
10. Failure of the Contractor to obtain prior authorization to relocate a computer may result in the Contractor's inability to perform functions of the contract for a period of time. CalVCB will not reimburse the Contractor for lost production time.

7. EQUIPMENT

- a. Written request and approval prior to purchase

The Contractor shall obtain prior written authorization from CalVCB in the acquisition of any/all equipment (capitalized assets), including "modular furniture", even though funding may have been previously requested and made part of the budget. CalVCB reserves the option of not reimbursing the Contractor for equipment purchases that are not approved in writing prior to purchase.

The Contractor shall submit the request for equipment purchases on the County Purchase Request Form (Attachment VII to this contract) to the attention of the County Liaison and Support Section, California Victim Compensation Board, P. O. Box 3036, Sacramento, CA 95812-3036.

If new equipment is purchased the County will be sent an Asset Identification Form (Attachment IX) and affix an asset tag to the equipment.

- b. Purchase of Information Technology Equipment

Costs for providing information technology equipment (as defined in State Administrative Manual section 4819.2) including input and output devices with software as well as monthly maintenance fees and installation, as deemed necessary by CalVCB, shall be provided and/or reimbursed by CalVCB. Specifically, if CalVCB purchases equipment, then CalVCB will configure, install,

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

and provide support for equipment and operating software. If the Contractor purchases equipment, then the Contractor is responsible for its own configuration, installation, and support of those purchases, which may involve the purchase of a maintenance service agreement with the vendor. The Contractor is responsible for budgeting dollars through this contract to cover those support and/or maintenance service agreement costs. CalVCB is not a party to such contract.

All equipment purchased or reimbursed under this contract, regardless of whether CalVCB or the Contractor purchased it, shall be the property of CalVCB and shall be identified with a state identification number. The Contractor shall ensure that no one other than a staff person who performs duties under this contract uses CalVCB equipment. The Contractor is responsible for maintaining equipment in such fashion that any warranties are not voided.

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

The Contractor agrees to apply security patches and upgrades, and keep virus software up-to-date on any machine on which CalVCB data may be used.

CalVCB requires the Contractor to purchase a maintenance agreement that provides on-site support within 24 hours.

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

CalVCB reserves the right to access and audit all IT assets purchased or reimbursed under this agreement, including software, equipment, and computers, to ensure they are patched, used and operating in a manner consistent with State policy and the terms of this contract. All personal computers should be using the following hardware, or an approved equivalent, which is the current standard for CalVCB:

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

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

The Contractor shall obtain prior written authorization from CalVCB prior to installing any equivalent or additional software on CalVCB purchased or reimbursed equipment. Requests should be immediately directed to the CLASS Manager or designee.

**8. OPERATING EXPENSES**

- a. The Contractor may charge expenses to various line-item allocations as part of its operating expenses such as rent, utilities, postage, and telephone, etc. Such expenses are generally identified as "direct costs". The Contractor shall ensure that expenses that are classified as "direct cost" 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 awarded.

The Contractor shall obtain written approval prior to modifications being made to the line items under the operating expense category such as an increase to rent or offsetting savings from one line item to another. Requests should be directed to the CLASS Manager or designee.

**9. PERFORMANCE PERIOD AND CONTRACT RENEWAL**

The period of performance for the contract shall be for three (3) years from July 1, 2018 through June 30, 2021.

**10. INVENTORY**

Electronic Data Processing equipment, capitalized assets and non-capitalized assets, reimbursed or paid for under this contract shall remain the property of CalVCB and shall bear identification tags supplied by CalVCB. The Contractor shall prepare an equipment inventory listing using the County Inventory Form (Attachment VIII) in July of each year for the term of this contract. The completed forms shall be submitted by e-mail to their assigned CLASS analyst. Inventory listings not submitted by end of July each year shall result in a delay in payment of submitted invoices.



**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

In the event of termination of this agreement, CalVCB shall take possession of its property. The Contractor shall hold those items identified in the inventory list in storage until CalVCB retrieves its property. Payment of storage and retrieval shall be the responsibility of CalVCB.

CalVCB reserves the right to request current and complete inventory listings, and to remotely access, for audit purposes, all IT equipment procured through this contract.

Any other arrangements for disposal or surplus of equipment requires approval from CalVCB's Business Services Branch. Counties must contact their assigned CLASS analyst to initiate this process.

**11. CONFIDENTIALITY OF RECORDS**

- a. All financial, statistical, personal, technical and other data and information relating to the State's operations which are designated confidential by the State and made available to the Contractor in order to carry out this agreement, or which become available to the Contractor in carrying out this agreement, shall be protected by the Contractor from unauthorized use and disclosure through observance of the same or more effective procedural requirements as applicable to the State. This includes the protection of any extractions of CalVCB's confidential data for another purpose. Personally identifiable information shall be held in the strictest confidence, and shall not be disclosed except as required by law or specifically authorized by CalVCB (refer to CalVCB Information Security Policy Memo 17-008, Attachment I to this contract). This shall apply regardless of whether or not the services for such staff persons are paid for by CalVCB.
- b. CalVCB's Custodian of Records in Sacramento shall be notified when an applicant or applicant's representative requests a copy of any document in or 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, Deputy Executive Officer, or Legal Division.

CalVCB's Legal Division in Sacramento is to be immediately notified of any request made under the Public Records Act (PRA) (Gov. Code, §6250, et. seq.) for information received or generated in the performance of this contract. No record shall be disclosed pursuant to any such request unless authorized by CalVCB's Legal Division.

- c. The Contractor shall ensure that all staff are informed of and comply with the requirements of these provisions and any direction given by CalVCB. The Contractor shall complete and submit with their signed contract a Confidentiality Statement

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

signed by each employee performing work under this contract (Attachment II to this contract)

- d. The Contractor shall be responsible for any unauthorized disclosure by Contractor staff persons performing duties under this contract and shall indemnify, defend and hold harmless the State, its officers, agents and employees from any and all claims, losses, damages, penalties, fines, and attorney fees resulting from the unauthorized disclosure of CalVCB records by such staff persons.
- e. The Contractor shall annually submit to CalVCB the confidentiality statements (see Attachment II) signed by each staff member performing services under this contract, whose salary or a portion thereof is paid through this contract, or who supervises staff members performing services under this contract. Confidentiality statements must be submitted within ten (10) business days of the start date of new staff. The Contractor should submit via mail, email or fax confidentiality statements for all staff no later than July 30 of each year. Access to CalVCB claims management database will be granted upon receipt of the signed confidentiality statements.

To mail requests and correspondence related to this section of the contract, send to: County Liaison and Support Section, California Victim Compensation Board, P.O. Box 3036, Sacramento, CA 95812-3036.

- f. The Contractor will forward any PRA request or Information Practices Act (IPA) request received related to provision of services under this contract to CalVCB's Legal Division. The Contractor will not take action on any PRA or IPA request for CalVCB records without obtaining prior permission from CalVCB's Legal Division.

**12. SUBPOENAS**

The Contractor is not the Custodian of Records for any of the materials it creates or receives pursuant to this contract. The Contractor shall post a notice in its receiving department or other appropriate place stating that all subpoenas for CalVCB records must be personally served on the California Victim Compensation Board at 400 R Street, 5<sup>th</sup> Floor, Sacramento, CA, 95811, Attn: Legal Division. The Contractor must notify anyone attempting to serve a subpoena for records of this requirement. The Contractor may also contact CalVCB's Legal Division at 916-491-3605 for further assistance.

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

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

**13. RETENTION OF RECORDS**

The Contractor shall retain all documents and records in hard copy related to applications entered into Cares2 for one year from the date the document is received. The Contractor shall retain all soft copies until confirmed uploaded into Cares2

The Contractor shall retain all records relating to the operation of this contract, including but not limited to, payroll, time-keeping, accounting records and electronic records, for seven years from the date the record is created. All electronically retained documents shall have the same legal effect as an original paper document.

**14. SUBCONTRACTING**

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 his responsibilities and obligations hereunder. 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 Contractor. The Contractor's obligation to pay its subcontractors is an independent obligation from the State's obligation to make payments to the Contractor. As a result, the State shall have no obligation to pay or to enforce the payment of any monies to any subcontractor.

**15. TERMINATION FOR CONVENIENCE**

CalVCB or the Contractor reserves the right to terminate this agreement upon thirty (30) days written notice to the other. In such an event, the Contractor shall be compensated for actual costs incurred in accordance with the terms of the agreement up to the date of termination. Invoicing of the above-mentioned costs shall be submitted to CalVCB within thirty (30) calendar days of the date of termination.

**16. 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.

**17. COMPLIANCE WITH CALVCB POLICY**

The Contractor shall ensure that all staff assigned work related to this contract, review and comply with the requirements of CalVCB policies, including the CalVCB Fraud Policy (Attachment III), CalVCB Information Systems Security and Confidentiality Policy (Attachment X), Password Policy (Attachment VI), the CalVCB Privacy Policy (Attachment XII) and the Acceptable use of Technology Resources (Attachment XI).

**EXHIBIT D  
SPECIAL TERMS AND CONDITIONS**

CLASS will provide copies of the policies to the Contractor on July 1, along with an Acknowledgement of Policies Form (Attachment V), which must be signed by each county employee under this contract and returned to CLASS within 30 days of receipt.

**18. SECURITY AND PRIVACY COMPLIANCE**

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

- a. Attempt to access the Cares2 application from any location other than their assigned work location. Remote access is only permitted with prior written approval from the CalVCB Deputy Executive Officer of the Victim Compensation Division.
- b. Share individual login ID and password with anyone else.
- c. Allow their computer to remember a password to the Cares2 application.
- d. Walk away from their computer without locking the screen (Ctrl+Alt+Delete).
- e. Leave documents with Personal Identifiable Information (PII) unattended on printers or fax machines, or in cubicles, offices or conference rooms.
- f. Visit untrusted websites or open any attachments or links from untrusted email.
- g. Uninstall or disable anti-virus software and automatic updates.
- h. Install any unauthorized or unlicensed software.
- i. Plug a mobile phone, personal USB drive or other peripheral device into the network system or desktop computer.
- j. Disclose any PII information to unauthorized users.
- k. Send any PII via email. Staff should use application numbers, bill numbers and initials only (if necessary). Staff should use encrypted email if they must send email containing PII information.
- l. Any virus attacks, security violations, and privacy breaches, should be immediately reported to the Contractor's Information Security Officer, the Contractor's CLASS Liaison and the CLASS Manager.

# 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 (CaIVCB) 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 CaIVCB rules related to information security.

## Information Security Program

The CaIVCB has established an Information Security Program to protect the confidentiality, availability, integrity, and privacy of CaIVCB information and supporting assets. The Information Security Program provides an integrated set of requirements that complement the CaIVCB 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 CaIVCB ITD Chief Information Officer.

The ISO will develop and implement policies, practices, and guidelines that protect the confidentiality, availability, and integrity of all CaIVCB 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 CaIVCB 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 CaIVCB information system.

## Data Ownership

All information assets have a Data Owner who is assigned by CaIVCB 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 CaIVCB information assets are classified by their Data Owner according to the confidentiality of the information and its importance to CaIVCB 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 CaIVCB operations.

## Information System Security Practices

All CaIVCB information systems and information system infrastructure elements will have specific practices, guidelines, and procedures that govern their operation relative to information security. All CaIVCB 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 [iso@calvcb.org](mailto:iso@calvcb.org).

## Distribution List

All CalVCB staff

## CaIVCB Confidentiality Statement

### Purpose of Confidentiality Statement

It is the policy of the Victim Compensation Board (CaIVCB) that all computerized files and data that contain CaIVCB 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 CaIVCB. I also acknowledge that it is the policy of CaIVCB to ensure that all information is secured as set forth in the CaIVCB Information Security Policy, Memo number 17-008 and that all CaIVCB employees and contractors must respect the confidentiality of CaIVCB data by not disclosing any files or data accessible to them through their employment, contract, or affiliation with CaIVCB.

### State Employees and Contractors

*Initial each section.*

I, SP 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-CaIVCB business related reason.
- Never attempt to access, use, disclose, or modify information, including my own, for any non-CaIVCB 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 CaIVCB without prior authorization from the Executive Officer, Deputy Executive Officer, or Legal Counsel.
- Log off of computer access to CaIVCB data and information when not using it.
- Never remove confidential information from my work site without prior authorization from the Executive Officer, Deputy Executive Officer, or Legal Counsel.
- Never disclose personal information regarding anyone other than the requestor unless authorized to do so by the Executive Officer, Deputy Executive Officer, or Legal Counsel. "Personal Information" means any information that identifies or describes an individual, including but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history, or statements made or attributed to the individual.

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

I, SM acknowledge that as a state employee or individual performing work pursuant to a contract with CalVCB, I am required to know whether the information I have been granted access to is confidential and to comply with this statement and the CalVCB Information Security Policy, Memo Number 17-008. If I have any questions, I will contact CalVCB's Legal Office or Information Security Officer.

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

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

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

## Certification

I have read, understand, and agree to abide by the provisions of the Confidentiality Statement and the CalVCB 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. 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.

Stephanie Medina  
Signature

4/30/18  
Date

Stephanie Medina  
Name (Print)

## CalVCB Confidentiality Statement

### Purpose of Confidentiality Statement

It is the policy of the Victim Compensation Board (CalVCB) that all computerized files and data that contain CalVCB client information, as well as all information and documents associated with such files and data, are "confidential" and shall not be disclosed except as required by law or specifically authorized by CalVCB. I also acknowledge that it is the policy of CalVCB to ensure that all information is secured as set forth in the CalVCB Information Security Policy, Memo number 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.

### State Employees and Contractors

*Initial each section.*

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

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

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

I, JD acknowledge that as a state employee or individual performing work pursuant to a contract with CalVCB, I am required to know whether the information I have been granted access to is confidential and to comply with this statement and the CalVCB Information Security Policy, Memo Number 17-008. If I have any questions, I will contact CalVCB's Legal Office or Information Security Officer.

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



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

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

## Certification

I have read, understand, and agree to abide by the provisions of the Confidentiality Statement and the CalVCB 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. 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.

*Tina Spencer*  
Signature

5-8-2018  
Date

TINA SPENCER  
Name (Print)



**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.

**Fraud Policy**

Memo Number: 17-004

## How to Report Fraud

Any employee who suspects fraud or has received an external fraud complaint shall immediately report it to his or her supervisor/manager and should not attempt to conduct the investigation personally. Managers must complete an Investigation Referral Form (available on Boardnet), and submit it to the Deputy Executive Officer of their division for referral to the Provider Evaluation Team (PET).

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

There are four reporting options available for external complainants:

1. Send an email to the fraud hotline at [FraudHotline@victims.ca.gov](mailto:FraudHotline@victims.ca.gov)
2. Call the toll-free fraud hotline at 1 (855) 315-6083
3. Write to the Legal Division at 400 R Street, Sacramento, CA 95811
4. Fax the complaint to (916) 491-6409

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 CaIVCB.

All information received in the course of a fraud investigation is treated as confidential to the extent permitted by law. CaIVCB 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. CaIVCB employees must report any alleged reprisal, retaliation, threat or similar activity immediately.

In order to maintain the integrity of the investigation, CaIVCB 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

**Fraud Policy**

Memo Number: 17-004

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.

# Training Request



## 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 State 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*

## Leadership Requirements

- New Supervisor *80 hours within 6 months of appointment or no later than term or probationary period.*
- New Manager *40 hours within 12 months of appointment. If new to state service, 80 hours of basic supervisory training is also required.*
- Ongoing Leadership *20 hours biennially*
- CEAs *20 hours within 12 months of appointment. If new to state service, 80 hours of basic supervisory training is also required.*
- On the Job *To receive credit, must be pre-approved by HR and complete On the Job Training Verification form.*

## 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/Manager Signature \_\_\_\_\_  
Date

\_\_\_\_\_  
DEO/Executive Officer Signature \_\_\_\_\_  
Date

\_\_\_\_\_  
Budget Officer Signature \_\_\_\_\_  
Date

# Training Section Confirmation

Accepted for Class Dates \_\_\_\_\_

Processed by Training Office/Enrolled \_\_\_\_\_

Date \_\_\_\_\_

**Note:** These dates are subject to change. An e-mail confirming class date will be sent one week prior to the scheduled class.

## Course Evaluation *For Training Coordinator Use*

Received back?

\_\_\_\_\_  
Sent Date

After attending the class, fill out a Course Evaluation (available on Boardnet, under Training) and submit it to the Training Coordinator within two weeks after the class.

## California Victim Compensation Board Acknowledgement of Polices

### 1. Fraud Activities Statement (Attachment III)

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

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

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

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

### 2. Acceptable Use of Technology Resources (Attachment XI)

I have read, understand, and agree to abide by the provisions of CalVCB's Acceptable Use of Technology Resources Policy (Memo 17-005)

### 3. Privacy Policy (Attachment XII)

I have read, understand, and agree to abide by the provisions of CalVCB's Privacy Policy (Memo 17-010)

### 4. Password Policy (Attachment VI)

I have read, understand, and agree to abide by the provisions of CalVCB's Password Policy (Memo 17-012)

### 5. Incompatible Work Activities

I have read, understand, and agree to abide by the provisions of the Exhibit D, Section 2, 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

Stephanie Medina  
County Employee's Signature

Stephanie Medina  
Typed or Printed Name

Meg. R. R.  
Manager/Supervisor Signature

Megan Rheinschild  
Type or Printed Name

Santa Barbara  
County

4/30/18  
Date

VVC Claims Specialist  
Classification Title

5/04/18  
Date

VW Program Director  
Classification Title

VC-8059  
Contract Number



## California Victim Compensation Board Acknowledgement of Polices

### 1. Fraud Activities Statement (Attachment III)

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

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

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

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

### 2. Acceptable Use of Technology Resources (Attachment XI)

I have read, understand, and agree to abide by the provisions of CalVCB's Acceptable Use of Technology Resources Policy (Memo 17-005)

### 3. Privacy Policy (Attachment XII)

I have read, understand, and agree to abide by the provisions of CalVCB's Privacy Policy (Memo 17-010)

### 4. Password Policy (Attachment VI)

I have read, understand, and agree to abide by the provisions of CalVCB's Password Policy (Memo 17-012)

### 5. Incompatible Work Activities

I have read, understand, and agree to abide by the provisions of the Exhibit D, Section 2, 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

Tina Spencer

County Employee's Signature

Tina Spencer

Typed or Printed Name

Megan Rheinschild

Manager/Supervisor Signature

Megan Rheinschild

Type or Printed Name

Santa Barbara

County

5-8-2018

Date

VVC Claims Specialist

Classification Title

Date

VW Program Director

Classification Title

VC-8059

Contract Number

# 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 CaIVCB 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 Standards 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 CaIVCB 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 CaIVCB internal systems, applications, or resources.

### **Remote Access Passwords**

Remote Access Passwords shall be used to authenticate a user's access to CaIVCB 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 CaIVCB, 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 Security Table 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 CaIVCB Information Security Policy.

## Who to contact for questions

For any questions about this Memo please contact your supervisor or manager, or the CaIVCB Information Security Officer by e-mail at [InfoSecurityandPrivacy@victims.ca.gov](mailto:InfoSecurityandPrivacy@victims.ca.gov).

## COUNTY PURCHASE REQUEST FORM

(formerly the Equipment Purchase Justification  
 Authorization Request Form)

	The following information must be provided in order for authorization to be granted for the purchase of equipment through the County's contract. As stated in the contract, <b>all equipment purchases must be justified by the requesting County and approved by CalVCB.</b> If the request is not approved by CalVCB, the purchase <u>will not</u> be authorized for payment through the contract. A separate form must be completed for each piece of equipment being requested.		
<b>1.</b>	<b>COUNTY CONTACT INFORMATION</b>		
	County:	Contract Number:	Fiscal Year Funded:
	Contact Name:	Address:	Phone Number:
	Email:		
<b>2.</b>	<b>EQUIPMENT REQUEST</b>		
	Submission of this form is not a guarantee of equipment approval. CalVCB's CRC/JP Analyst, Business Services Branch (BSB) Analyst, and Information Technology Division (ITD) 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. <i>Note: Acquisition of an equipment maintenance plan is the responsibility of the County, and may be funded through the contract.</i>		
	Equipment Type:	Make:	Model: Cost:
	Software: (e.g., Windows 7, Microsoft Office Suite)		Cost:
	Equipment Maintenance Plan: (describe terms/pricing)		Cost:
	Explain how payment for the equipment shall be made: (approved in contract budget, purchased by VCP, other)		
<b>3.</b>	<b>PURCHASE JUSTIFICATION</b>		
	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 CRC/JP Analyst to provide additional information.		
<b>4.</b>	<b>COUNTY AUTHORIZATION</b>		
	By signing this form, the County Coordinator/Supervisor agrees that the information provided is accurate and true, and that the equipment/software is necessary to conduct State business. The coordinator/supervisor is also accepting responsibility to ensure that upon receipt, the asset tag provided for this equipment will be properly affixed to the equipment.		
	County Coordinator/Supervisor Signature:		Date:
<b>5.</b>	<b>PURCHASE APPROVAL</b>		
	If the purchase is approved, a fully executed copy of the County Purchase Request Form will be returned to the County Contact (see Page 2). The County may then proceed with their equipment purchase. Carefully review the approval as alternative equipment may have been authorized.		

**NOTE: Retain a copy of this document for further processing. After equipment has been acquired, the County will be required to complete the CalVCB Asset Identification Form. This form will provide CalVCB with the information needed to document the equipment specifications and serial number. Upon receipt by CalVCB, an asset tag will be assigned and sent to the County with further instructions.**



### COUNTY PURCHASE REQUEST FORM

(formerly the Equipment Purchase Justification  
 Authorization Request Form)

<b>For CalVCB Staff Use Only:</b>			
The CRC/JP 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 CRC/JP Analyst will serve as the liaison between the County Contact and/or the BSB/ITD Analysts for clarifying or resolving any issues. Upon review/approval by the CRC/JP Analyst and the CRC/JP Manager, the form will be forwarded to BSB for further review and processing.			
<b>CRC/JP Analyst Staff Comments:</b>  <div style="border: 1px solid black; height: 100px; width: 100%;"></div>			
This request is: <input type="checkbox"/> Approved <input type="checkbox"/> Denied	CRC/JP Analyst Name:	Date:	
CRC/JP Manager's Signature (required)	Signature:	Date:	
The BSB Analyst is responsible for determining if the equipment requested is proportionate to staff size, available through State contracts, best pricing and/or quotes obtained, etc. If this request is for IT equipment, components or software, BSB will forward to ITD for additional review/approval.			
<b>BSB Approval / Comments</b> (include Approved Changes or Denial details in this section):  <div style="border: 1px solid black; height: 100px; width: 100%;"></div>			
This request is: <input type="checkbox"/> Approved <input type="checkbox"/> Approved w/Changes <input type="checkbox"/> Denied	Approved by (BSB Analyst):		Date:
BSB Manager's Signature (required)	Signature:	ITD Review/Approval Required? Yes <input type="checkbox"/> No <input type="checkbox"/>	
The ITD Analyst is responsible for determining if the IT equipment requested is compatible with CalVCB equipment and/or meets all requirements to interface with the CalVCB's database, and may also determine if the equipment requested is proportionate to staff size, available through State contracts, best pricing and/or quotes obtained, etc. ITD and BSB will consult regarding equipment replacement, as necessary.			
<b>ITD Approval/Comments</b> (include Approved Changes or Denial details in this section):  <div style="border: 1px solid black; height: 100px; width: 100%;"></div>			
This request is: <input type="checkbox"/> Approved <input type="checkbox"/> Approved w/Changes <input type="checkbox"/> Denied	Approved by (ITD Analyst):		Date:
ITD Manager's Signature (required for IT purchases only)	Signature:	Date:	

**COUNTY PURCHASE REQUEST FORM:  
INSTRUCTIONS AND RESPONSIBILITIES**

**County Staff Responsibilities - Request**

1. County staff will complete each section of the County Purchase Request Form (form) and obtain County authorization.
2. The County will then submit the form to their assigned CRC/JP Analyst.

**CRC/JP Analyst Responsibilities - Review**

1. CRC/JP 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 is returned** to the County with instructions on how to proceed (i.e., complete cost, provide justification, etc.).
2. CRC/JP Manager will either sign and approve the form, or deny the request and return the form to the County with an explanation of the denial.
3. If approved, CRC/JP Analyst will send the signed, approved form to BSB for further processing.

**BSB Staff Responsibilities - Process**

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

**ITD Staff Responsibilities - Process**

1. ITD will verify that the purchase is appropriate/compatible and authorize the IT equipment by checking "Approved".
  - If alternate equipment is recommended, ITD will check "Approved w/Changes" and explain the reason for the change.
  - If the equipment request is not approved, ITD will check "Denied".
2. ITD will route the form to BSB for further processing.
3. Upon receipt, BSB will make a copy of the form and return it to the appropriate CRC/JP Analyst.

**CRC/JP Analyst Responsibilities - Status**

1. The CRC/JP 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. Once the new equipment is received, County staff will complete a State Asset Identification Form and submit it within 10 business days to their assigned CRC/JP Analyst.
2. An asset tag(s) will be sent from CalVCB to County staff once the equipment has been received.
  - A BLUE asset tag will be issued for non-IT equipment; a RED asset tag will be issued for IT equipment.
3. County staff will affix the asset tag(s) to the new equipment.

**Annual Inventory:** In July each fiscal year, County staff must submit a completed County Inventory Form which details all equipment purchased with CalVCB funds. This form must be returned to their assigned CRC/JP Analyst.

## CalVCB County Inventory Form

Attachment VIII

In accordance with the California Victim Compensation Board (CalVCB) contract with the County, the CalVCB Inventory Form must be completed and returned to CalVCB in July of each year.

Please complete all requested information. The only assets to be inventoried on this form are those purchased by CalVCB or with funds from CalVCB. For a list of assets that must be inventoried, please see details at the bottom of this form. For any questions on this form, please contact your CRC/JIP Analyst.

Return the completed form to your assigned analyst.

County Name	CalVCB Contract Number	Date	Address	Contact Information						
				<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Name:</td> <td></td> </tr> <tr> <td>Phone Number:</td> <td></td> </tr> <tr> <td>Email Address:</td> <td></td> </tr> </table>	Name:		Phone Number:		Email Address:	
Name:										
Phone Number:										
Email Address:										

### Asset Inventory

*Asset Type	Location	Serial Number	Model	Manufacturer	Asset Tag #	Comments

\*The following assets must be inventoried: IT Assets (computer, monitor, copier, fax machine, desktop or network printer, scanner, laptop) Non-IT Assets (shredder, recorder, TV, any type of furniture - chair, bookcase, cart, credenza, file cabinet, hutch, etc.)

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

## CalVCB Asset Identification Form

As required by the State Administrative Manual and the County contracts, all assets purchased with State funds must be properly identified and inventoried, and an asset tag affixed to the asset. 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 CRC/JP analyst.

<b>County Name</b>	<b>Contract Number</b>	<b>Address</b>
<b>County Contact Name</b>	<b>Phone Number</b>	<b>Email Address</b>

<b>ASSET INFORMATION</b>	
(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>	

\*The following examples represent the types of assets that must be inventoried: IT Assets: computer, monitor, copier, fax machine, desktop or network printer, scanner, laptop, etc. Non-IT Assets: shredder, recorder, TV, all furniture – chair, bookcase, cart, credenza, file cabinet, hutch, etc.

<b>COUNTY ACKNOWLEDGEMENT</b>	
<p>A complete accounting of all assets and corresponding asset tags must be provided to CalVCB in July of each Fiscal Year. Counties must use the <u>County Inventory Form</u> provided with their contract (see Contract Attachments) to account for and report all assets purchased with CalVCB funds. The County Coordinator/Supervisor understands and accepts responsibility for submission of a complete and accurate County Inventory Form for the current Fiscal Year.</p>	
<p>By signing below, you acknowledge that all asset tags have been properly affixed to equipment purchased with CalVCB funds, and that an accounting of all assets will be reported at the end of the Fiscal Year, as indicated above:</p>	
County Coordination/Supervisor (required):	Date:

<b>ASSET TAG</b>	
Asset Tag(s) Provided to CRC/JP Analyst By:	Asset Tag(s) Sent to County By:
BSB/ITD Analyst: _____ Date: _____	CRC/JP Analyst: _____ Date Sent: _____
<p>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.</p>	
<b>Asset Tag Number</b> To be provided by CalVCB	<div style="border: 1px solid black; width: 100px; height: 100px; margin: auto; display: flex; align-items: center; justify-content: center;"> <span style="font-size: 2em; color: gray;">ASSET TAG</span> </div>

Non-IT = Blue Asset Tag      IT = Red 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

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

\*The following examples represent the types of assets that must be inventoried: IT Assets: computer, monitor, copier, fax machine, desktop or network printer, scanner, laptop, etc. Non-IT Assets: shredder, recorder, TV, all furniture – chair, bookcase, cart, credenza, file cabinet, hutch, etc.

## 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 CaIVCB approved hardware and software and never download from the internet or upload from home.
- Not use CaIVCB 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 CaIVCB 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 CaIVCB reserves the right to review electronic files, electronic messages, internet data and usage at its facility, and those files and messages stored on CaIVCB systems may be disclosed under the California Public Records Act, discovered in legal proceedings, and used in disciplinary actions.

<u>Stephanie Medina</u>	<u>Santa Barbara D.A., SP002</u>	
User Name (Print)	Division or Unit	
<u>Stephanie Medina</u>	<u>4/22/18</u>	<u>(805) 568-2405</u>
User Signature	Date	Phone Number
<u>Meg Rice</u>	<u>5/4/18</u>	<u>805 568-2408</u>
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.

## 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.

<u>TINA SPENCER</u>	<u>JPOB3</u>	
User Name (Print)	Division or Unit	
<u>Tina Spencer</u>	<u>5-8-2018</u>	<u>805-934-6978</u>
User Signature	Date	Phone Number
<u>M. R.</u>	<u>5-16-2018</u>	<u>805-568-2408</u>
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.

# Acceptable Use of Technology Resources

---

**Memo Number: 17-005**

Date Issued: 1/11/17

Supersedes: 15-003

Effective Date: Immediately

Expires: Indefinite

Issued By: Information Technology Division

## Purpose

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

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

## Policy

It is the policy of the CalVCB that:

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

## Applicability

This Policy applies to:

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

**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 CaIVCB Information Security Officer (ISO).

## User Responsibilities

- Act in the best interest of the CaIVCB by adhering to this Policy.
- Use discretion when using CaIVCB information technology assets.
- Access only the CaIVCB 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 CaIVCB Help Desk via email at [helpdesk@calivcb.org](mailto:helpdesk@calivcb.org) 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 CaIVCB 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 CaIVCB will investigate all alleged violations and take appropriate action.

## Compliance

All employees must read the *CaIVCB 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 CaIVCB Policies

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

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



## Contact

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

# 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 (CaIVCB) from actions that would:

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

## Policy

It is the Policy of CaIVCB that:

- All personal, and personally identifiable information (PII) collected by CaIVCB is necessary for the organization to perform its function.
- CaIVCB 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, CaIVCB 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 CaIVCB. 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 CaIVCB.
- 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 CaIVCB.
- 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 CaIVCB Privacy Officer.

## Acceptable Use

Official CaIVCB 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

## POLICY MEMO



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

## Other Applicable CalVCB Policies

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

## Contact

For any questions about this Policy, please contact your immediate manager/supervisor or Information Security & Privacy Officer at \_\_\_\_\_

## Distribution

All CalVCB staff

# 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 CaIVCB 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 \_\_\_\_\_ 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 \_\_\_\_\_ 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 \_\_\_\_\_ 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 \_\_\_\_\_ 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 CaIVCB 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 CaIVCB internal systems, applications, or resources.

### **Remote Access Passwords**

Remote Access Passwords shall be used to authenticate a user's access to CaIVCB 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 CaIVCB, 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 \_\_\_\_\_ 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 \_\_\_\_\_.