SCO ID: 7870-S23011

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
S23-011	VCB-7870

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

CONTRACTING AGENCY NAME

California Victim Compensation Board

CONTRACTOR NAME

County of San Francisco

2. The term of this Agreement is:

START DATE

July 1, 2023

THROUGH END DATE

June 30, 2026

3. The maximum amount of this Agreement is:

$0.00

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

Exhibits	Title	Pages
Exhibit A	Scope of Work	5
Exhibit B	Budget Detail and Payment Provisions	2
Exhibit C *	General Terms and Conditions	GTC 04/2017
Exhibit D	Special Terms and Conditions	9
Attachment 1	Revolving Fund Procedures	4
Attachment 2	Confidentiality Statement	3
Attachment 3	Acceptable Use of Technology Resources	5
Attachment 4	Acknowledgement of Policies	1
Attachment 5	Information Security Policy	6
Attachment 6	Information Systems Security and Confidentiality Acknowledgement	2
Attachment 7	Fraud Policy	3
Attachment 8	Password Policy	6
Attachment 9	Privacy Policy	4
Attachment 10	Board Resolution	

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

SCO ID: 7870-S23011

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

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
S23-011	VCB-7870

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

CONTRACTOR

CONTRACTOR NAME (if other than an individual, state whether a corporation, partnership, etc.)
County of San Francisco

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

PRINTED NAME OF PERSON SIGNING	TITLE

CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME
California Victim Compensation Board

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

PRINTED NAME OF PERSON SIGNING	TITLE
Lynda Gledhill	Executive Officer

CONTRACTING AGENCY AUTHORIZED SIGNATURE	DATE SIGNED

CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	EXEMPTION (If Applicable)
	SCM Vol 1 section 4.04 (A)(2)

EXHIBIT A
SCOPE OF WORK

1. This Agreement is entered between County of San Francisco (Contractor) and the California Victim Compensation Board (CalVCB).

2. The purpose of this Agreement is to establish a process by which the Contractor may pay expenses on an emergency basis when the claimant would suffer substantial hardship if the payment was not made and when the payment would help the claimant with an immediate need.

3. Services shall be provided during the term of July 1, 2023, or upon final approval from CalVCB, whichever occurs later, through June 30, 2026. No work shall begin before that time. The services shall be provided during the working hours of 8:00 AM through 5:00 PM, Monday through Friday, excluding State holidays. At the beginning of each fiscal year the Contractor shall provide a list of scheduled holidays for the coming year. The Contractor shall obtain approval from the Joint Powers (JP) County Liaison Unit Manager in advance for any temporary changes in schedule or operating hours. The JP County Liaison Unit Manager shall approve all requests for overtime in advance.

4. The services shall be performed throughout the State of California designated sites as agreed upon by CalVCB and Contractor.

5. The project representatives during the term of this Agreement will be:

STATE AGENCY California Victim Compensation Board	**CONTRACTOR** County of San Francisco
Name: Lynda Gledhill	Name: Brooke Jenkins
Phone: 916-491-3501	Phone: 628-652-4000
Fax: 916-491-6435	Fax: 628-652-4101
Email: Lynda.Gledhill@victims.ca.gov	Email: Brooke.Jenkins@sfgov.org

Direct all inquiries to:

STATE AGENCY California Victim Compensation Board	**CONTRACTOR** County of San Francisco
Unit: Joint Powers County Liaison	Unit: District Attorney/Victim Services Unit
Attention: Jacqueline Hom	Attention: Monifa Willis, PMHNP-BC
Address: 400 R Street, Suite 400 Sacramento, CA 95811	Address: 350 Rhode Island Street, North Building, Suite 400N, San Francisco, CA 94103
Phone: 916-491-3691	Phone: 628-652-4114

EXHIBIT A
SCOPE OF WORK

Fax: 916-491-6435	Fax: 628-652-4101
Email: Jacqueline.Hom@victims.ca.gov	Email: Monifa.Willis@sfgov.org

Either party may change any portion of the above contact information by providing thirty (30) days written notice of the change to the other party. No amendment of this agreement is needed to make such a change.

6. The CalVCB and County of San Francisco agree:

   A. Contractor shall pay emergency expenses pursuant to Government Code section 13952.5, subdivision (c)(3) in the categories listed below according to the Revolving Fund Procedures, Attachment 1.

      1) Payment of verified funeral/burial expenses;
      2) Payment of verified relocation expenses;
      3) Payment of verified crime scene clean-up expenses; and
      4) Payments of other verified emergency losses with the approval of the JP County Liaison Unit Manager.

   B. The Contractor shall pay emergency expenses using its revolving fund for applications and bills related to crimes that occurred in the following location: County of San Francisco.

      Emergency expenses will be paid in additional counties as directed by the JP County Liaison Unit Manager or designee.

   C. For emergency awards, the Contractor shall receive and verify applications and requests for reimbursement according to the procedures established by the California Victim Compensation Board Policy and Procedure Manual, known as the WikiManual or its replacement, available to Contractor staff with access to the Compensation and Restitution System (Cares2), the CalVCB automated claims management system. Upon verification, the Contractor shall issue payments from the revolving fund for allowed emergency expenses. The Contractor shall then use CalVCB claims management system to issue a payment to replenish the revolving fund in accordance with the process set out in the Revolving Fund Procedures, Attachment 1 and any other subsequent procedures required by CalVCB. The Contractor shall not implement additional stipulations against this Agreement which hinders the claimant from receiving funds when an immediate need for payment of an expense has been verified.

EXHIBIT A
SCOPE OF WORK

D. The Contractor shall also ensure staff who authorize emergency payments are different from staff who issue the emergency payments and adhere to proper separation of duties and internal controls.

   The Contractor staff shall not participate in criminal investigations or prosecution. The Contractor shall also ensure that the staff persons assigned to functions under this Agreement do not collect restitution or serve as a restitution specialist.

   In addition, the Contractor shall obtain CalVCB's prior written permission if staff persons assigned to functions under this Agreement will perform any other County functions.

E. The Contractor shall establish and enforce procedures to ensure that funds paid under this Agreement are released only to the person authorized by the claimant to receive the funds or to the provider of services or for qualified commodities paid under this Agreement.

   CalVCB and the Contractor shall comply with all applicable State and Federal requirements. In compliance with Internal Revenue Code 6041 (26 U.S.C.A. § 6041), CalVCB shall issue the Contractor a Miscellaneous Income (Form 1099-MISC) at the end of the calendar year stating the amount that the Contractor received as payee from CalVCB that calendar year. The Contractor shall be responsible for issuing a Form 1099- MISC to each provider paid through the use of Revolving Funds, in accordance with Federal requirements no later than January 31st, of the following year. In accordance with CalVCB procedures, the Contractor shall submit a Request for Taxpayer Identification Number and Certification (Form W-9) or a Payee Data Record (Std. 204) to CalVCB for all providers to be paid through the CalVCB claims management database.

F. The Contractor shall exercise internal control over the issuance of funds and requests for reimbursement of funds to replenish the account.

G. The Contractor shall make a reasonable attempt to collect any overpayments made from its revolving fund according to the Revolving Fund Procedures, Attachment 1.

H. The Contractor shall use all forms and processes required by CalVCB as stated in the Revolving Fund Procedures, Attachment 1.

I. The Contractor shall only use information collected under this Agreement for the purpose of verifying and adjudicating claims.

EXHIBIT A
SCOPE OF WORK

J. The Contractor will use the Cares2, the CalVCB automated claims management system, to perform the work under this Agreement. The Contractor shall ensure that all staff performing duties under this Agreement comply with CalVCB statutes, regulations, guidelines, procedures, and processes.

K. The Contractor shall maintain the highest customer service standards and shall ensure that claims are processed accurately and efficiently, that recipients of services receive prompt responses to their inquiries and are treated with sensitivity and respect. The Contractor shall demonstrate and apply trauma-informed principles and practices when communicating verbally and in writing with recipients of services. Should CalVCB communicate to the Contractor any complaint or concern about the foregoing, the Contractor shall respond to CalVCB within a reasonable time as requested by CalVCB.

L. In compliance with the CalVCB Continuity Plan and in the event of a statewide or local emergency, within 30 calendar days from the execution of the Agreement, the Contractor will provide the name and emergency cellular contact information for the designated person responsible to maintain the services of the Revolving Fund (RF) account agreement to the JP-Invoice@victims.ca.gov email account.

M. Upon execution of this Agreement and within 30 calendar days, the Contractor shall submit, to the JP County Liaison Unit Manager for approval, the Contractor's Description of Revolving Fund Procedures. These procedures shall include a written description of the procedures for operating the revolving fund. The description shall include a list of all personnel authorized to request a disbursement from the revolving fund and a list of all personnel authorized to make such a disbursement. The description shall also include a complete explanation of the manner in which the revolving fund is operated, the timeframe for the issuance of any payment from the fund, the time frame for any payment to be considered void if not presented for payment and copies of any forms that are used in the distribution of the funds. Failure to submit the Revolving Fund Procedures within 45 calendar days shall place the Contractor out of Agreement compliance. If any changes are made to the Contractor's Description of Revolving Fund Procedures, the Contractor shall notify CalVCB prior to the changes taking effect for approval.

7. Incompatible Work Activities

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

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

EXHIBIT A
SCOPE OF WORK

B. Use information obtained while doing work under this Agreement for personal gain or the advantage of another person.

C. Disclose any confidential information except as required by law or authorized by CalVCB. Confidential information includes, but is not limited to, information about applicants, applications and documents associated with applications.

D. Provide or use the names of persons or records of the CalVCB for a mailing list which has not been authorized by CalVCB.

E. Represent himself or herself as a CalVCB employee.

F. Take any action with regard to a CalVCB claim or restitution matter with the intent to obtain private gain or advantage.

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

H. Knowingly initiate any contact with a claimant, person for whom restitution may be sought, or person against whom restitution may be collected, unless the contact is for the purposes of carrying out the services under this Agreement and is done in an appropriate manner.

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

It shall be the Contractor's responsibility to ensure that every staff person assigned to provide contracted services to CalVCB is made aware of and abides by this provision. If an assigned staff person is unwilling or unable to abide by this provision, the staff person should no longer be assigned to perform the services required by the Agreement. Any questions should be directed to CalVCB's Legal Office at (916) 491-3605.

8. If there is any conflict between Attachments 1 through 10, and any provisions in the STD 213 Agreement, including Exhibits A, B, C, and D, the provisions in the Agreement shall prevail over the Attachments.

EXHIBIT B
BUDGET DETAIL AND PAYMENT PROVISIONS

1. Revolving Fund

   To establish a revolving fund account, CalVCB advanced the Contractor a total of $75,000.00, which consists of $75,000.00 in fiscal year 2001/2002, authorized by Government Code section 6504 to pay qualifying claims identified in Exhibit A.

2. Budget Contingency Clause

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

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

3. Reporting Revolving Fund Use

   A. In order to perform an accurate reconciliation of the revolving fund, CalVCB requires that each month the Contractor shall submit a written accounting of the disbursements and reimbursements made to the Contractor's revolving fund account.

      Required documentation shall be submitted to the JP County Liaison Unit designee at JP-Invoice@victims.ca.gov and CalVCB Accounting Inbox at AccountingMailbox@victims.ca.gov, by the tenth (10^{th}) day of each month.

   B. Required documentation shall include:

      1) Revolving Fund Disbursement Log

         a) The spreadsheet for the Revolving Fund Disbursement Log shall be provided by CalVCB.

      2) Bank Statements or General Ledger Report

         a) If statements are comingled with other funds, then a General Ledger

EXHIBIT B
BUDGET DETAIL AND PAYMENT PROVISIONS

a) If statements are comingled with other funds, then a General Ledger report with only revolving fund transactions is required.
b) Debit information should include the county check number. This check number will be reconciled with the Revolving Fund Disbursement Log to determine the application identification number.
c) Credit information should also include deposit information that states what claim payments are being deposited by application identification number and a copy of the corresponding warrant from the State Controller's Office (SCO).

3) Summary of any discrepancies e.g. voided transactions, errors in posting, overpayments, etc.

C. According to the process set out in the Revolving Fund Procedures, Attachment 1, the Contractor shall submit a report within (30) days after the end of the fiscal year that details all transactions in the revolving fund, including but not limited to the following information: beginning and ending balance of the fund, the number of applications, number of bills, total amount disbursed from the revolving fund, total number of bills by service type (e.g., funeral/burial, relocation expense, etc.), total amount paid by service type, and percentage disbursed based on service type.

EXHIBIT C
GENERAL TERMS AND CONDITIONS

General Terms and Conditions (GTC 04/2017)

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

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

1. Settlement of Disputes

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

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

2. Termination

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

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

3. Termination For Convenience

   CalVCB or the Contractor reserves the right to terminate this Agreement upon thirty (30) days written notice to the other party. In such an event, the Contractor shall return all Revolving Fund monies to be deposited into the CalVCB Restitution Fund and will 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.

4. Amendments

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

5. Subcontracting

   All subcontracting must comply with the requirements of the State Contracting Manual, Volume 1, Section 3.06. Nothing contained in this agreement or otherwise shall create any contractual relation between the State and any sub-contractors, and no

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

subcontract shall relieve the Contractor of their responsibilities and obligations herein. The Contractor agrees to be as fully responsible to the State for the acts and omissions of its subcontractors and of persons either directly or indirectly employed by any of them as it is for the acts and omissions of persons directly employed by 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 moneys to any subcontractor.

6. Executive Order N-6-22 Russia Sanctions

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

7. Americans with Disabilities Act

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

8. Regulations and Guidelines

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

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

accordance with federal and state labor laws.

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

10. Performance Assessment

A. CalVCB may assess and evaluate the Contractor's performance based on data from Cares2. This includes completed disposition information, inventory, notes, amended orders, uploaded documents, and all activity.

B. CalVCB reserves the right to revoke the logon of any Contractor whose performance is consistently poor or below average based on the performance criteria used by CalVCB or who does not comply with the Agreement provisions. CalVCB may monitor performance under the Agreement and report performance to the Contractor and their supervisor/manager.

C. CalVCB may set performance and production expectations or goals for the Contractor related to the fulfillment of the services in this Agreement. The expectations may include but are not limited to: specific time frames for completion of work; specific amount of work to be completed within given time frames; specific standards for the quality of work to be performed; and the amount of restitution imposed. CalVCB may provide written notice of the performance and production expectations to the Contractor and their supervisor/manager. If the Contractor fails to achieve the performance and production expectations set by CalVCB, CalVCB may reduce the amount of the contract or terminate the Agreement.

11. Confidentiality Of Records

All financial, statistical, personal, technical and other data and information relating to the State's operations which are designated confidential by the State and made available to the Contractor in order to carry out this Agreement, or which become available to the Contractor in carrying out this Agreement, shall be protected by the Contractor from unauthorized use and disclosure through observance of the same or more effective procedural requirements as are applicable to the State. This includes the protection of any extractions of CalVCB's confidential data for another purpose.

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

Personal identifiable information (PII) shall be held in the strictest confidence and shall not be disclosed except as required by law or specifically authorized by CalVCB in accordance to the CalVCB Information Security Policy, Attachment 5.

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, or Chief Counsel.

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

The Contractor shall ensure that all staff are informed of and comply with the requirements of this provision and any direction given by the CalVCB. The Contractor shall complete and submit a signed Information Systems Security and Confidentiality Acknowledgement, Attachment 6, to:

California Victim Compensation Board
Joint Powers County Liaison Unit
JP-Invoice@victims.ca.gov

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

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

California Victim Compensation Board
Joint Powers County Liaison Unit
JP-Invoice@victims.ca.gov

12. Retention of Records

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

A. Application Records

The Contractor shall retain all documents related to applications entered into the Compensation and Restitution System (Cares2), the CalVCB automated claims management system, for one year from the date the document is received. After one year, the Contractor shall contact the JP County Liaison Unit to make arrangements for the documents to be destroyed consistent with the CalVCB Records Retention schedule.

B. Administration and Fiscal Records

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

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

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

13. Subpoena

The Contractor is not the Custodian of Records for any of the materials it creates or receives pursuant to this Agreement. The Contractor shall post a notice in its receiving department or other appropriate location stating that subpoenas for all records from CalVCB must be personally served on CalVCB at the California Victim Compensation Board, Attn: Legal Division at 400 R Street, Ste. 500, Sacramento CA 95811. The Contractor may also contact the Legal Division at (916) 491-3651 for assistance or questions.

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

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

14. Compliance with CalVCB Policies

The Contractor shall ensure that all staff review and comply with the requirements of

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

the Acceptable Use of Technology Resources (Attachment 3), Privacy Policy (Attachment 9), Password Policy (Attachment 8), and Fraud Policy (Attachment 7). Staff are required to fill out and submit signed copies of the CalVCB Confidentiality Statement (Attachment 2), the Information Systems Security and Confidentiality Acknowledgement (Attachment 6), and Acknowledgement of Policies (Attachment 4) to:

California Victim Compensation Board
Joint Powers County Liaison Unit
JP-Invoice@victims.ca.gov

The Contractor shall annually submit to CalVCB the Information Systems Security and Confidentiality Acknowledgement, Attachment 6, signed by each staff member performing services under this Agreement, whose salary or a portion thereof is paid through this Agreement, or who supervises staff members performing services under this Agreement. Confidentiality statements must be submitted within ten (10) business days of the start date of new staff and annually each year by mail, email or fax. Access to the CalVCB claims management system will be granted upon receipt of the signed confidentiality statement.

15. Utilization of Computer System

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

16. Security and Privacy Compliance

The Contracted 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

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

assigned work location, this includes restrictions on working remotely unless written authorization is obtained from the JP County Liaison Unit Manager.

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.

E. Leave documents with personal identifiable information (PII) unattended on printers or fax machines, or in cubicles, offices or conference rooms.

F. Disclose any PII information to unauthorized users.

G. 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.

H. Visit untrusted websites or open any attachments or links from untrusted email.

I. Uninstall or disable anti-virus software and automatic updates.

J. Install any unauthorized or unlicensed software.

K. Plug a mobile phone, personal USB drive or other peripheral device into the network system or desktop computer.

Any virus attacks, security violations, suspected security incidents, or privacy breaches should be reported immediately to your county Information Security Officer (ISO) and your supervisor. You must also notify the JP County Liaison Unit Manager and copy CalVCB's IT Help Desk and ISO by sending an email to: ServiceDesk@victims.ca.gov and to InfoSecurityOffice@victims.ca.gov.

The Contractor and all staff with access to CalVCB computer systems are required to complete Information Security and Privacy Training, including at a minimum training regarding Social Engineering and Phishing, Privacy and Password Protection, Browsing Safely, and Ransomware at least annually.

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

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

to CalVCB computer systems must complete the training within thirty (30) days from the date of hire.

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

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

All other terms and conditions under this Agreement shall remain the same, in full force, and effect.

17. Information Technology Equipment and Software

A. The Contractor is responsible for the purchase, configuration, installation, and support of all personal productivity computer equipment used for CalVCB data processing activities.

B. The Contractor shall certify that it has appropriate systems and controls in place to ensure that computer software is acquired, operated, and maintained in a manner that complies with applicable copyrights.

C. The Contractor agrees to apply all security patches and upgrades and keep anti-virus software executed and up to date on any machine CalVCB data may be accessed or used. The Contractor shall apply appropriate end point protection, data encryption, and data loss prevention technologies. 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.

D. CalVCB reserves the right to access and audit all IT assets including software, equipment, and computers, to ensure they are patched, used, and operated in a manner consistent with State policy and the terms of this Agreement.

E. All personal computers should use the following hardware, or an approved equivalent, which is the current standard for CalVCB:

1) Intel current Generation Multi-Core i7 Processor
2) 16 GB RAM or better
3) 256 GB Hard Drive or better
4) Network Port

EXHIBIT D
SPECIAL TERMS AND CONDITIONS

5) USB Port(s)
6) 24" Flat Panel Monitor
7) USB Keyboard
8) USB Mouse or Trackball

F. All personal computers should use the following software, or an approved equivalent, which is the current standard for CalVCB:

1) Current Windows Enterprise Operating System
2) Current version of Microsoft Edge or Google Chrome
3) Windows Media Player or equivalent
4) Current supported version of Microsoft Office
5) Current supported version of Adobe Acrobat Reader or Professional
6) Current anti-virus protection software

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

18. Return of Revolving Funds

CalVCB reserves the right to request, upon thirty (30) days written notification, the return of all revolving fund monies to be deposited into CalVCB Restitution Fund.

REVOLVING FUND PROCEDURES

1. Document Substantial Financial Hardship and Immediate Need

A. The Revolving Fund may be used to pay urgent or unexpected expenses that are allowed by CalVCB statutes, regulations and policies. Typically, these expenses are considered through the Emergency Award (EA) process. Emergency awards can only be allowed in cases where there would be substantial financial hardship if an award were not paid right away and/or where there is an immediate need for payment to the claimant or the provider on behalf of the claimant.

B. Substantial financial hardship means that without the emergency award the claimant cannot provide for the necessities of life including, but not limited to:

1) Shelter
2) Food
3) Medical care or
4) Personal safety

C. The inability to pay for funeral and burial expenses or crime scene clean up expenses without the emergency award can constitute substantial financial hardship.

D. The amount awarded depends on the claimant's immediate need. Pay just those compensable expenses that, if not paid immediately, would cause a substantial financial hardship.

2. Contact the Provider

A. Payments from the Revolving Fund should be verified:

1) To be a substantial financial hardship to the claimant,
2) To be an immediate need and
3) That the provider will not provide services unless payment is received immediately

B. Prior to making payments to a provider of service on behalf of the claimant, local county staff will contact the provider by phone to assess whether they are willing to wait for payment through the regular claims process.

C. Document the conversation in the Compensation and Restitution System (Cares2), specifying whether or not the provider is willing to wait for the payment.

3. Assess Eligibility

A. Prior to making a payment from the Revolving Fund review the application and associated documents (per instructions in the CalVCB online manual) to make a preliminary assessment regarding the eligibility of the application.

B. Whenever possible determine eligibility of the application prior to issuing the Revolving Fund payment, however, if circumstances do not allow for a complete eligibility assessment, follow the instructions found in the CalVCB online manual for making an emergency award.

C. Do not issue a Revolving Fund payment in a case where issues that may bar eligibility are clearly evident. Consult with the Joint Powers (JP) County Liaison Unit if assistance is needed in reviewing eligibility issues.

4. Issuing and Documenting the Revolving Fund Payment

A. Prior to issuing a Revolving Fund payment, all reimbursement sources must be reviewed. If necessary, contact the Probate, Settlement Recovery, and CRC Unit (PSRU) for authorization to pay the bill prior to issuance. Per instructions in the manual, document interactions with PSRU in Cares2. Escalate emergency claims by contacting your JP County Liaison Unit analyst for assistance.

B. Confirm who needs to be paid (claimant or provider on behalf of the claimant). If needed, obtain a W-9 form from the provider, which includes either the provider's Federal Tax Identification Number (FIN) or Social Security Number (SSN). This information is used to issue a future Form 1099.

C. Payment authorization documents must be scanned into Cares2 or every Revolving Fund transaction. The format of the authorization documents may differ from county to county but must contain at a minimum:

1) CalVCB Application Number
2) Date of request
3) Nature of request (including amount and payee)
4) Evidence of substantial financial hardship or immediate need
5) Status of application
6) Signature of claims specialist making the request
7) Signature of Victim Assistance Center Director or authorized designee approving request
8) Signature of person issuing the check
9) The person making the request, the person approving the request and the person issuing the check must be three different people

D. Staff must enter a note into the Cares2 application summary for each Revolving Fund transaction. The note must be written according to the following format:

REVOLVING FUND PAYMENT: Payment in the amount of *[amount]* to *[payee]* has been issued from the Revolving Fund on date *[date].* The Revolving Fund was used because *[document reason including substantial financial hardship/immediate need and the provider's unwillingness to wait for payment through CaRES, if applicable].* Copies of Revolving Fund authorization documents *[authorization form and a copy of the check if available]* scanned into CaRES *[date].*

5. Reimbursing the Revolving Fund

A. The JP County Liaison Unit office should reimburse the Revolving Fund within 20 days of the time the Revolving Fund check was issued in order to keep funds flowing back into the Revolving Fund.

B. Reimbursement to the Revolving Fund must also be documented in the application summary with a note in the following format:

REVOLVING FUND REIMBURSEMENT Bill ID no. BXX-XXXXX: This payment of *[amount]* to the *[County Emergency Fund]* is reimbursement for the Revolving Fund payment made in the amount of *[amount]* to *[payee]* on *[date].*

6. Revolving Fund Disbursement Log

A. Use the Revolving Fund Disbursement Log provided by CalVCB to document all outgoing and incoming Revolving Fund transactions. The log shall include, but is not limited to, the following information:

- The date of the transaction
- Application and bill identification numbers
- Claimant's initials
- Payee name and federal tax identification number,
- The county warrant number disbursed
- The State warrant number used to reimburse the fund
- Paid amount

B. The disbursement log must reflect an accurate beginning balance from July 1, 2023, and should be cumulative for the year. Outstanding items from the prior fiscal year may be included on the July 2023 log in order to provide an accurate reconciliation.

7. Bank Statements or General Ledger Report

A. If statements are comingled with other funds, then a General Ledger report with only revolving fund transactions is required.

B. Debit information should include the county check number. This check number will be reconciled with the Revolving Fund Disbursement Log to determine the application identification number.

C. Credit information should also include deposit information that states what claim payments are being deposited by application identification number and a copy of the corresponding check from the State Controller's Office (SCO).

D. Summary of any discrepancies e.g. voided transactions, errors in posting, etc. Assign one person in the county office to maintain the Revolving Fund Disbursement Log to ensure that all required information is documented properly and reimbursements are requested promptly.

8. Submission of the Revolving Fund Disbursement Log and Bank Statement or General Ledger Report

A. The Revolving Fund Disbursement Log and bank statement or general ledger must be submitted by the 10th day of the month following the reporting month. The Revolving Fund Disbursement Log must be submitted to:

CalVCB Accounting Division	AccountingMailbox@Victims.ca.gov
JP Revolving Fund	JP-Invoice@Victims.ca.gov

9. Overpayments

A. If an overpayment is identified as a result of an error the Contractor made when issuing the Revolving Fund payment or when making the subsequent reimbursement to the county, the Contractor is responsible for making a reasonable attempt to collect the amount of the overpayment.

- The Contractor shall report any overpayments or suspected overpayments to JP-Invoice@VICTIMS.CA.GOV at CalVCB as soon as the overpayments are identified.

- The Contractor shall follow overpayment procedures established for processing overpayment. If the Contractor has made a reasonable attempt to recover the overpayment but the overpayment was not recovered, then CalVCB will pursue collection of the overpayment from the overpaid party. For a detailed description of overpayment procedures refer to the CalVCB manual.

Confidentiality Statement

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

Purpose of Confidentiality Statement

It is the policy of the California Victim Compensation Board (CalVCB) that all computerized files and data that contain CalVCB client information, as well as all information and documents associated with such files and data, are "confidential" and shall not be disclosed except as required by law or specifically authorized by CalVCB.

I also acknowledge that it is the policy of CalVCB to ensure that all information is secured as set forth in the CalVCB's Information Security Policy, Memo Number 17-008 and that all CalVCB employees and contractors must respect the confidentiality of CalVCB data by not disclosing any files or data accessible to them through their employment, contract, or affiliation with CalVCB.

CalVCB Employees and Contractors

Initial each section.

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

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

    1. The request for information is from an applicant or the applicant's authorized representative regarding his or her own application,
    2. The disclosure is for the purpose of verifying claims and the applicant has provided a signed authorization to release information, or
    3. Are authorized to disclose the information by the Executive Officer, Deputy Executive Officer, or Legal Counsel.

Confidentiality Statement

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

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

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

I, _____ acknowledge that the unauthorized access, inspection, use, or disclosure of confidential information is a violation of applicable laws, including but not limited to, the following: Government Code sections 13954, 7923.755, and 19990, subdivision (c), Civil Code section 1798, et seq., and Penal Code section 502. I further acknowledge that unauthorized access, inspection, use, disclosure, or modification of confidential information, including my own, or any attempt to engage in such acts can result in:

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

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

Confidentiality Statement

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

Certification

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

I also understand that improper use of CalVCB files, data, information, and systems could constitute a breach of contract. I further understand that I must maintain the confidentiality of all CalVCB files, data, and information once my employment, contract, or affiliation with CalVCB ends.

If I am a State employee, this signed Certification will be retained in my Official Personnel File in Human Resources.

If I am a contractor, I understand that it is my responsibility to share these contract provisions with any staff under my supervision and ensure that they comply with its provisions. This signed Certification will be retained by the Contract Manager and Business Services Unit as part of the contract file.

Signature

Date

Name (Print)

Contract Number (If applicable)

POLICY MEMO

Acceptable Use of Technology Resources

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

Purpose

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

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

Policy

It is the policy of the CalVCB that:

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

Applicability

This Policy applies to:

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

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

Management Responsibilities

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

User Responsibilities

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

Requests for Exception

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

Acceptable Activities

The following are examples of acceptable activities:

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

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

Restriction on the Use of State IT Resources

The following are examples of unacceptable activities:

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

Incident Reporting

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

Violations

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

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

Compliance

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

Authority

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

Other Applicable CalVCB Policies

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

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

Contact

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

STATE OF CALIFORNIA

Acknowledgement of Policies

VCB-22-10013 (Rev. 03/2023)

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

ATTACHMENTS	
☐ Confidentiality Statement (Attachment 2)	☐ Fraud Policy (Attachment 7)
☐ Acceptable Use of Technology Resources (Attachment 3)	☐ Password Policy (Attachment 8)
☐ Information Security Policy (Attachment 5)	☐ Privacy Policy (Attachment 9)
☐ Information Systems Security and Confidentiality Acknowledgement (Attachment 6)	

INCOMPATIBLE WORK ACTIVITIES

☐ I have read, understand, and agree to abide by the provisions of Exhibit A, Section 7, 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.

_____ _____

Contractor Name Contract Number

_____ _____

Contractor Signature Date

POLICY MEMO

Information Security Policy

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

Purpose

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

Information Security Program

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

Responsibility

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

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

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

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

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

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

Compliance

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

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

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

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

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

Risk Management

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

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

Life Cycle Planning

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

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

Awareness and Training

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

Physical Security

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

Contingency and Disaster Preparedness

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

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

Incident Handling

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

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

Identification and Authentication

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

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

Access Control

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

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

Audit Trail

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

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

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

Data Ownership

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

Information Classification

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

Information System Security Practices

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

Authority

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

Contact

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

Distribution List

All CalVCB staff

Information Systems Security and Confidentiality Acknowledgement

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

I understand that I must:

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

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

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

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

Filing Instructions

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

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

Fraud Policy

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

Purpose

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

Policy

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

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

Definition

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

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

How to Report Fraud

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

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

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

There are four reporting options available for external complainants:

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

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

Investigations

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

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

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

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

Contacts

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

POLICY MEMO

Password Policy

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

Policy

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

Purpose

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

Requirements

Passwords shall always be kept confidential.

Passwords shall not be viewable on a display device.

Password Standards

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

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

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

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

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

Changing Passwords

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

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

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

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

Initial Passwords

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

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

Initial User Passwords shall be unique to each user.

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

Session Inactivity Protection

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

Lockout

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

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

Stored or Transmitted Passwords

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

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

Business Partners Passwords

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

User Passwords

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

Remote Access Passwords

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

Administration Passwords

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

Stored and Embedded Passwords

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

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

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

Embedded passwords shall be contained within the system or application.

Default Passwords

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

Exception Approval

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

Password Standards

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

Password Character Type Table

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

Guidelines

Automatic System Enforcement

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

Encrypted Transmission

Passwords should be encrypted when transmitted across internal networks.

Writing Down Passwords

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

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

Minimizing the Number of User Passwords

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

Change Embedded Password

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

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

Account Names for Stored and Embedded Passwords

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

Compliance and Authority

Refer to the CalVCB Information Security Policy.

Who to contact for questions

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

POLICY MEMO

Privacy Policy

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

Purpose

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

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

Policy

It is the Policy of CalVCB that:

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

Definition

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

Applicability

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

Management Responsibility

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

Staff Responsibility

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

- Properly dispose of PII.

Privacy Officer Responsibility

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

Acceptable Use

Official CalVCB business needs only.

Monitoring

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

Incident Reporting

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

Violations

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

Compliance

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

Authority

- Government Code sections 11019.9, 13952 to 13954

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

Other Applicable CalVCB Policies

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

Contact

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

Distribution

All CalVCB staff

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