ATTACHMENT I

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:

        i. Shelter
        ii. Food
        iii. Medical care or
        iv. 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:

        i. To be a substantial financial hardship to the claimant,
        ii. To be an immediate need and
        iii. 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 Cares2, specifying whether or not the provider is willing to wait for payment.

3. **Assess eligibility**

    a. Prior to making a payment from the Revolving Fund review the application and associated documents (per instructions in the CalVCP 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 CalVCP 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 the County Liaison and Support Section 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 Revenue and Recovery Branch for authorization to pay the bill prior to issuance. Per instructions in the manual, document interactions with RRB in Cares2. Escalate emergency claims by contacting your County Liaison and Support Section (CLASS) 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 CaRES for every Revolving Fund transaction. The format of the authorization documents may differ from county to county but must contain at a minimum:
    i. CalVCB Application Number
    ii. Date of request
    iii. Nature of request (including amount and payee)
    iv. Evidence of substantial financial hardship or immediate need
    v. Status of application
    vi. Signature of claims specialist making the request
    vii. Signature of Victim Assistance Center Director or authorized designee approving request.
    viii. Signature of person issuing the check.
    ix. 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 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, 2020, and should be cumulative for the year. Outstanding items from the prior fiscal year may be included on the July 2020 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. Also 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 Log and Bank Statement or General Ledger Report

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

CalVCB Accounting Division		AccountingMailbox@victims.ca.gov
CLASS Manager	Dionne Bell-Rucker	Dionne.bell-rucker@victims.ca.gov
CLASS Liaison	Johnny Wong	johnny.wong@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.

i. The Contractor shall report any overpayments or suspected overpayments to County Liaison and Support Section (CLASS) at CalVCB as soon as the overpayments are identified.

ii. 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.

ATTACHMENT II

CONTRACTOR'S DESCRIPTION OF REVOLVING FUND PROCEDURES

County Name: San Francisco	Prepared by: Maria Miguel
Original Revolving Fund Contract Award: $75,000.00	Contract Number: S20-020
Date: 4/13/2020	Phone: (415) 551-9539

The contractor shall submit a written description of the procedures for operating the Revolving Fund (Attachment II to this contract). 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 fund is operated, the timeframe for any warrant to be considered void if not presented for payment and copies of any forms that are used in the distribution of funds.

Feel free to attach additional pages or documentation.

The following personnel are authorized to request a disbursement from the Revolving Fund

Delia Montiel (Advocate Supervisor)

Karima Baptiste (Advocate Supervisor)

Patricia Barragan (Advocate)

Gretel Chuquipul (Advocate)

Abby Cordova (Advocate)

Patricia Cuellar (Advocate)

Melissa Curiel (Advocate)

Sai Douangsawang (Advocate)

Amanda Esquivel (Advocate)

Giles Feinberg (Advocate)

Willie Gray (Advocate)

Peter Huynh (Advocate)

Melissa McNair (Advocate)

Israel Murillo (Advocate)

Selina Perez (Advocate)

Priscilla Portillo (Advocate)

Maria Reynoso (Advocate)

Rose Robinson (Advocate)

Kimberly Rodriguez (Advocate)

Jovan Thomas (Advocate)

Thu Tran (Advocate)

Edgar Zamudio (Advocate)

Francesca Zarate (Advocate)

ATTACHMENT II

Personnel authorized to make a disbursement from the Revolving Fund:

Gena Castro-Rodriguez (Deputy Chief/Victim Services Division)

Paige Allmendinger (Acting Assistant Deputy Chief/Victim Services Division)

Sheila Arcelona (Assistant Chief/Finance and Administration)

Eugene Clendinen (Chief/Administration and Finance)

Lorraine Gi (Finance Division Analyst)

Manner in which Fund is operated: See Revolving Fund Procedures (*attached*)

Timeframe for any warrant considered to be void if not presented for payment: Check becomes stale after 6 months

Exhibit 1

CITY AND COUNTY OF SAN FRANCISCO

OFFICE OF THE DISTRICT ATTORNEY

CHESA BOUDIN
District Attorney

VICTIM SERVICES
628-652-4100

Victims of Crime Compensation Program
Revolving/Burial Funds (San Francisco)

Control #: _____ ☐ Funeral/Burial ☐ Crime Scene Clean-Up ☐ Emer. Reloc./DV ☐ Emer. Reloc./SA

A. To be completed by Victim Services – Advocacy Team

Date of Request: _____ Advocates Name: _____

Police Report/Case No: _____

Claim #: _____
(if no claim #, attach claim form & police report.)

Name of Claimant: _____

Name of Victim: _____

Check Payable To:

Amount Requested: _____
(please attach invoice/lease/etc.)

Service Provider's Name: _____

Payment Address: _____

_____

Contact Person: _____

Telephone No.: _____

Victim Advocate's Comments/Notes: _____

_____

Reviewed by Victim Services – Advocacy Team, Deputy Director:
☐ Addresses Reviewed Initial & Date →: _____

Reviewed by Victim Services – Claims Team, Supervisor:
☐ Addresses Reviewed Initial & Date →: _____

B. To be completed by Finance/Accounting

Attach PeopleSoft Document and attached a copy of the printed check.

C. To be completed by Victim Services - Claims Team

Data input by: _____

Comments/Notes: _____

Revolving Fund Procedures:

- ❑ Advocate fills out the CalVCB application with Claimant and collects all supporting documentation.

 Advocate fills out a SFDA **Victims of Crime Compensation Program Revolving/Burial Funds (San Francisco)** coversheet (Exhibit 1), then submits the coversheet and all supporting documents to Advocate Supervisor, Assistant Deputy Chief or Deputy Chief for review and approval.

- ❑ Once approved, the Advocate Supervisor, Assistant Deputy Chief or Deputy Chief will sign the coversheet, staple all items together and return the packet to the Advocate.
- ❑ Advocate then walks the approved packet to the Claims Unit and turns the documents over to the Claims Lead Specialist (Monica Wheaton-Howell) or Claims Supervisor (Maria Miguel) for review.
- ❑ Claims Supervisor or Claims Lead Specialist will:

1) Review the application, police report, bills/contracts.
2) Research in **Cares** for potential duplicates.
3) Contact Law Enforcement if additional clarification is needed.
4) Contact providers and verify submitted bills.
5) Once verification is complete, the Claims Supervisor or Claims Lead

- ❑ Specialist will sign the **Victims of Crime Compensation Program Revolving/Burial Funds (San Francisco)** coversheet (Exhibit 1) and return the packet to the Advocate.
- ❑ Advocate then obtains a Control number from our SFDA internal computer system, known as SFDA/VW Relocation Database, which generates a Control number, for tracking purposes.
- ❑ Advocates then submits the approved packet to the Financial Division Analyst (listed in section I).
- ❑ Finance Division Analyst reviews packet to ensure packet is complete and signed by a Supervisor in Advocacy Unit and a Supervisor or Lead in the Claims Unit, then processes payment.
- ❑ Finance Division Analyst reviews and approves payment in Finance system.
- ❑ Chief of Administration and Finance reviews and approves payment in Finance system.
- ❑ Once check has been cut, the Finance Division Analyst logs all Claim information onto CalVCB Revolving Fund Disbursement Log, makes a copy the check and contacts Advocate to pick up check.

ATTACHMENT III

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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

ATTACHMENT IV

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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.

dtyson	T077	
User Name (Print)	Division or Unit	
	4/10/2020	415-551-9588
User Signature	Date	Phone Number
Maria Miguel	4/10/2020	415-551-9539
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.

ATTACHMENT IV

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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.

Heidy Carlson	Victim Services	
User Name (Print)	Division or Unit	
	4/10/2020	415-551-9591
User Signature	Date	Phone Number
Maria Miguel	4/10/2020	415-551-9539
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.

ATTACHMENT IV

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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.

Monica Wheaton-Howell	SF T077	
User Name (Print)	Division or Unit	
Monica Wheaton-Howell	4/10/20	415 551-9590
User Signature	Date	Phone Number
Maria Miguel	4/10/20	415 551-9539
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.

ATTACHMENT IV

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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.

mmiguel	T077	
User Name (Print)	Division or Unit	
Maria Miguel	4/10/2020	415-551-9539
User Signature	Date	Phone Number
Jena Castro Rodriguez	4/13/20	415-420-4851
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.

ATTACHMENT IV

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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.

Ferdinand Laxamana	SF DAT	
User Name (Print)	Division or Unit	
	April 10, 2020	415-551-9597
User Signature	Date	Phone Number
Maria Miguel	4/10/2020	415-551-9539
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.

ATTACHMENT IV

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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.

Imani Carter	JP T077	
User Name (Print)	Division or Unit	
	4/10/2020	(415) 581 - 9818
User Signature	Date	Phone Number
Maria Miguel	4/10/2020	415-551-9539
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.

ATTACHMENT IV

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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.

Rommel Castelo	Victim Services Unit - Claims Department	
User Name (Print)	Division or Unit	
	4/10/2020	(415)551-9593
User Signature	Date	Phone Number
Maria Miguel	4/10/2020	415-551-9539
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.

ATTACHMENT V

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.

ATTACHMENT VI

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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

ATTACHMENT VII

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

Document Receiving Section (DRS) Imaged Document Confidential Destruct Policy

Memo Number: 17-
Date Issued:
Supersedes: 09-001
Effective Date: Immediately
Expires: Indefinite
Issued By: Executive Office

Purpose

It is the policy of the California Victim Compensation Board (CalVCB) to properly retain and dispose of documents scanned into the California Compensation and Restitution System (CaRES) in a timely manner to save storage and handling costs.

Authority

California Codes

- Penal Code Section 11106.1, 11106.2
- Evidence Code Section 1550–1553
- Government Code Section 12159–12179.1

Internal Organization of Standardization

- ISO 15489-1: Information and documentation, Records management, Part 1
- ISO/TR 15489-2: Information and documentation, Records management, Part 2

Policy

According to the California Codes, any document imaging system that does not permit additions, deletions, or changes to an original document, may be used as a photographic reproduction process to record documents, as long as a trusted system is utilize. A "trusted

system" means a combination of techniques, policies, and procedures for which there is no possible scenario in which a document retrieved from or reproduced by the system could differ substantially from the document that is originally stored. The CaRES claims management system is fully compliant with these requirements.

Based on these requirements, an original document that has been electronically imaged into CaRES can be destroyed when the following document guidelines and retention periods have been observed.

Document Guidelines

All documents received by the DRS are registered and batched with a batch header sheet and scanned in batches of like documents, such as new applications, bills, and include a batch header sheet. Visual quality controls are performed on each document uploaded into the CaRES system. The first quality control measure is performed by the individual scanning the documents; the second quality control is performed by the individual validating the document; the third quality control is performed by the individual uploading the documents into the CaRESCaRES system. Once quality control is complete and the batches are uploaded into the CaRES system, the paper batches are placed in boxes, labeled by batch type, and divided by date and time.

Retention Period

All paper documents that have been imaged and released into the CaRES system will be retained by the File Room for a period of twelve (12) months. This period is determined by adding twelve (12) calendar months to the date the documents were uploaded into the CaRES system. If a business unit requires an original document, they may retrieve it through the DRS within twelve (12) months of the original scan date. At the end of the twelfth month, the documents will be placed in designated confidential destruct bins in the File Room. The documents will be scheduled for onsite confidential destruction with a certified confidential shredding service.

If you have any questions, please contact Business Services Branch Manager, at (916) 491-3866.