Attachment I

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

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

CalVCB Confidentiality Statement

Purpose of Confidentiality Statement

It is the policy of the Victim Compensation Board (CalVCB) that all computerized files and data that contain CalVCB client information, as well as all information and documents associated with such files and data, are "confidential" and shall not be disclosed except as required by law or specifically authorized by CalVCB. I also acknowledge that it is the policy of CalVCB to ensure that all information is secured as set forth in the Information Security Policy, Memo number 17-008 and that all CalVCB employees and contractors must respect the confidentiality of CalVCB data by not disclosing any files or data accessible to them through their employment, contract, or affiliation with CalVCB.

State Employees and Contractors

Initial each section.

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

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

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

I, _____ acknowledge that as a state employee or individual performing work pursuant to a contract with CalVCB, I am required to know whether the information I have been granted access to is confidential and to comply with this statement and theB 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 1470 et seq, 6254.17, and 19990(c), Civil Code section 1798 et seq., and Penal Code section 502. I further acknowledge that unauthorized access, inspection, use, disclosure, or modification of confidential information, including my own, or any attempt to engage in such acts can result in:

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

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

CALIFORNIA
CalVCB
VICTIM COMPENSATION BOARD

Certification

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

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

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

Signature

4/3/19
Date

Alexandria Lucas
Name (Print)

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 400 R Street, Sacramento, CA 95811
4. Fax the complaint to (916) 491-6409

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

Investigations

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

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

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

INVESTIGATION REFERRAL FORM

Involved Division/County (check all that apply)

- ☐ Victim Compensation Division
  - ☐ Application Intake Section
  - ☐ Eligibility Determination Section
  - ☐ Benefit Determination Section
  - ☐ County Liaison and Support Section
  - ☐ Mental Health Section
  - ☐ Appeals Process Section
  - ☐ Policy, Planning and Research Section
  - ☐ Customer Service Section
- ☐ Administration Division
  - ☐ Human Resources Section
  - ☐ Information Technology Section
  - ☐ Business Services Section
- ☐ Fiscal Services Division
  - ☐ Budget Section
  - ☐ Accounting Section
  - ☐ Government Claims Program
  - ☐ Restitution Recovery Section
  - ☐ Liens & Overpayment Recovery Section
- ☐ Legislation & Public Affairs Division
  - ☐ Legislation Section
  - ☐ Regulations Section
  - ☐ Training Section
  - ☐ Communications & Outreach Section
- ☐ Joint Powers County
- ☐ Criminal Restitution Compact County

Nature of Complaint (check all that apply)

- ☐ Services not rendered
- ☐ Unnecessary services
- ☐ Excessive billing
- ☐ Double billing
- ☐ Upcoding and Unbundling
- ☐ Provider licensure issue
- ☐ Identity theft
- ☐ Forgery/alteration of documents
- ☐ Misappropriation of State assets
- ☐ Other (Please describe):

Complainant

☐ Employee ☐ Claimant ☐ Provider ☐ Attorney/Representative ☐ Other

Name and Title

Unit/Section (if applicable)

Contact Number

Date

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

INVESTIGATION REFERRAL FORM

Complaint Against

☐ Employee ☐ Claimant ☐ Provider ☐ Attorney/Representative ☐ Other

Name of the involved

Name(s) of other parties involved

Application Number and Any Associated Application Numbers (if applicable)

Application Processed By? ☐ Headquarters ☐ JP County

Dollar Amount Involved?

Type of Expenses Involved? ☐ MH ☐ Relocation ☐ I/S ☐Medical ☐ F/B ☐ Other

Date of Complaint Occurred?

Date of Complaint Discovered?

Complaint (Summary of the complaint – What did the person(s) involved do that you feel was fraudulent, etc.?) If applicable, send a copy of any documents that supports your complaint. If you do not have a copy of supporting documents, where can a copy be obtained?)

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

INVESTIGATION REFERRAL FORM

Approving Manager/Supervisor Signature (Name & Title)*

Unit/Section (if applicable)

Phone Number

Date

*Not required if you believe your supervisor is involved in the fraudulent activity.

Approving Deputy Executive Officer:

☐ Proceed to OAI ☐ Return to Requestor

Reason for Return:

Deputy Executive Officer Signature _____ Date _____

To assist in the processing of a complaint involving a CalVCP application, please ensure all necessary verifications are completed prior to submission.

California Victim Compensation Board
Acknowledgement of Policies

1. **Fraud Policy (Attachment III)**

   I have read, understand, and agree to abide by the provisions of the CalVCB's Fraud Policy (Memo 17-004). I understand that if an issue arises regarding these requirements during my daily work and I suspect dishonest or fraudulent activity, I should immediately notify my JP or CRC supervisor/manager and/or the CalVCB's Office of Audits and Investigations (OAI) for review. When the employee believes his or her supervisor/ manager is involved in the fraudulent activity, the employee should contact the OAI section directly.

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

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

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

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

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

3. **Privacy Policy (Attachment XII)**

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

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

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

5. **Incompatible Work Activities**

   I have read, understand, and agree to abide by the provisions of the Exhibit D, Section 14, 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

CRC Restitution Specialist Signature	**Date** 4/3/2019
Alexandria Loufas	Paralegal
Typed or Printed Name	**Classification Title**
Manager/Supervisor Signature	**Date**
Sharon Henry	Chief Deputy District Attorney
Type or Printed Name	**Classification Title**
Solano County	VC - 9085
County	**Contract Number**

INSTRUCTIONS FOR COMPLETING MONTHLY INVOICES

All costs in the following categories/subcategories should be included if they are necessary to perform the services under this agreement and provided for in the budget.

Personnel Expenses - Salaries and Wages
Salary is calculated as follows: Hourly Rate x Hours Worked x % Billed = Salary Billed. Salary cannot exceed actual amount paid out as listed on the back-up documentation.

Fringe Benefits
Benefits are calculated as follows: Salary billed x Benefit % = Benefit Billed.

Operating Expenses
The following items fall within this category: rent, utilities, postage, data processing, office supplies, telephone, insurance, training, travel, and expendable equipment. All items submitted must include a description or explanation of the expense, and a receipt, if necessary.

The following subcategories have special requirements as noted below. Rent
The rent subcategory is for facility rental. Indicate the number of square feet specified in the agreement as well as the rental amount. A receipt is not required.

Office Supplies
A request for office supplies in excess of $500 per PY requires a justification for the entire amount of expenditures. Receipts required.

Workers' Compensation Insurance
Workers' Compensation insurance may be billed to the county as an annual fee; however, it cannot be billed to the contract as an annual lump sum. Please divide the annual amount and bill monthly. Include back-up information detailing the charge.

Travel
All travel must be pre-authorized by CalVCB. Allowable expenses include transportation, lodging, meals and incidental items incurred by the Specialist to attend training classes, conferences, meetings, workshops or hearings. Out-of-state travel is not authorized.

The contractor may use either its own written travel and per diem policy or the state policy in accordance with State Administrative Manual Section 0700, but it cannot exceed the state's travel reimbursement rate.

Describe the purpose of the trip and list all personnel who made the trip. If applicable, show any computation if mileage is being claimed. For example, if the Specialist attended a conference in Sacramento, 100 miles @ 0.58 per mile = $58.00.

Expendable Equipment (Non-capitalized assets)
Expendable equipment includes equipment with an acquisition cost of $499 or less per unit (including tax, installation and freight) or with a useful life of less than five years. Provide a detailed description and indicate the number of pieces of equipment being purchased.

Equipment (Capitalized Assets)
Capitalized assets include equipment with an acquisition of $500 or more per unit (including tax, installation and freight) or with a useful life of five years or more. Examples of such equipment are copiers, personal computers (including monitors and CPU). Provide a detailed description and indicate the number of pieces of equipment being purchased.

Note
Although equipment is included in the budget, **ALL** equipment for which the county requests reimbursement from the California Compensation Board (CalVCB) must be requested in writing and approved in writing **prior to purchase**. All requests must be submitted on the **County Purchase Request Form** (Attachment VII). Further, CalVCB reserves the option of not reimbursing for equipment that is not requested and approved in writing prior to purchase.

COUNTY PURCHASE REQUEST FORM

(formerly the Equipment Purchase Justification Authorization Request Form)

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

1. COUNTY CONTACT INFORMATION

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

2. EQUIPMENT REQUEST

Submission of this form is not a guarantee of equipment approval. CalVCB's CRC/JP Analyst, Business Services Branch (BSB) Analyst, and Information Technology Division (ITD) Analyst, will verify the request and make recommendations based on appropriateness and pricing. Alternatives may be recommended. Incomplete forms will be returned to the County.
Note: Acquisition of an equipment maintenance plan is the responsibility of the County, and may be funded through the contract.

Equipment Type:	**Make:**	**Model:**	**Cost:**
Software: (e.g., Windows 7, Microsoft Office Suite)			**Cost:**
Equipment Maintenance Plan: (describe terms/pricing)			**Cost:**
Explain how payment for the equipment shall be made: (approved in contract budget, purchased by VCP, other)			

3. PURCHASE JUSTIFICATION

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

4. COUNTY AUTHORIZATION

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

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

5. PURCHASE APPROVAL

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

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

COUNTY PURCHASE REQUEST FORM

(formerly the Equipment Purchase Justification
Authorization Request Form)

For CalVCB Staff Use Only:

The CRC/JP Analyst is responsible for determining if the equipment/software is necessary for the County to conduct State business, and will also ensure that the form is complete, accurate, and contains the appropriate signature. The CRC/JP Analyst will serve as the liaison between the County Contact and/or the BSB/ITD Analysts for clarifying or resolving any issues. Upon review/approval by the CRC/JP Analyst and the CRC/JP Manager, the form will be forwarded to BSB for further review and processing.

CRC/JP Analyst Staff Comments:

This request is: ☐ **Approved** ☐ **Denied**	**CRC/JP Analyst Name:**	**Date:**
CRC/JP Manager's Signature (required)	**Signature:**	**Date:**

The BSB Analyst is responsible for determining if the equipment requested is proportionate to staff size, available through State contracts, best pricing and/or quotes obtained, etc. If this request is for IT equipment, components or software, BSB will forward to ITD for additional review/approval.

BSB Approval / Comments (Include Approved Changes or Denial details in this section):

This request is: ☐ **Approved** ☐ **Approved w/Changes** ☐ **Denied**		**Approved by (BSB Analyst):**	
BSB Manager's Signature (required)	**Signature:**	**Date:**	**ITD Review/Approval Required?** Yes ☐ No ☐

The ITD Analyst is responsible for determining if the IT equipment requested is compatible with CalVCB equipment and/or meets all requirements to interface with the CalVCB's database, and may also determine if the equipment requested is proportionate to staff size, available through State contracts, best pricing and/or quotes obtained, etc. ITD and BSB will consult regarding equipment replacement, as necessary.

ITD Approval/Comments (Include Approved Changes or Denial details in this section):

This request is: ☐ **Approved** ☐ **Approved w/Changes** ☐ **Denied**		**Approved by (ITD Analyst):**
ITD Manager's Signature (required for IT purchases only)	**Signature:**	**Date:**

COUNTY PURCHASE REQUEST FORM:

INSTRUCTIONS AND RESPONSIBILITIES

County Staff Responsibilities - Request

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

CRC/JP Analyst Responsibilities - Review

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

BSB Staff Responsibilities - Process

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

ITD Staff Responsibilities - Process

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

CRC/JP Analyst Responsibilities - Status

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

County Staff Responsibilities – Asset/Inventory

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

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

CalVCB Asset Identification Form

As required by the State Administrative Manual and the County contracts, all assets purchased with State funds must be properly identified and inventoried, and an asset tag affixed to the asset. To comply with these requirements, the County must complete the information provided below.

Upon completion, a copy of this form must be emailed to your assigned CRC/JP analyst.

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

ASSET INFORMATION

(To be completed by the County; use Page 2 for additional items)

***Asset Type**	
Location/Address	
Make/Model	
Serial Number	

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

COUNTY ACKNOWLEDGEMENT

A complete accounting of all assets and corresponding asset tags must be provided to CalVCB in July of each Fiscal Year. Counties must use the County Inventory Form provided with their contract (see Contract Attachments) to account for and report all assets purchased with CalVCB funds. The County Coordinator/ Supervisor understands and accepts responsibility for submission of a complete and accurate County Inventory Form for the current Fiscal Year.

By signing below, you acknowledge that all asset tags have been properly affixed to equipment purchased with CalVCB funds, and that an accounting of all assets will be reported at the end of the Fiscal Year, as indicated above:

County Coordination/Supervisor (required):	Date:

ASSET TAG

Asset Tag(s) Provided to CRC/JP Analyst By:		Asset Tag(s) Sent to County By:	
BSB/ITD Analyst:	Date:	CRC/JP Analyst:	Date Sent:

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

Asset Tag Number To be provided by CalVCB	ASSET TAG

Non-IT = Blue Asset Tag IT = Red Asset Tag

CalVCB County Inventory Form

In accordance with Exhibit D.10 of the California Victim Compensation Board (CalVCB) Criminal Restitution Compact (CRC) contract, the *CalVCB County Inventory Form* must be completed and returned to CalVCB by the end of each fiscal year, **July 15th**, and at the time of an equipment purchase. Please list all assets purchased by CalVCB *or* reimbursed by CalVCB. For a list of assets that must be inventoried, please see footnote.

Return completed form to CalVCB at: BSSSupport@victims.ca.gov

County	CalVCB Contract Number	Fiscal Year	Address	Contact Information
Solano County	VC-9085	FY19/20- FY 21/22	675 Texas Street,Ste 4500 Fairfield, CA 94533	Name: Alexandria Loufas Phone Number: 707-784-6808 Email Address: AELoufas@solanocounty.com

Asset Inventory

Asset Type*	Location	Serial Number	Model	Manufacturer	Asset Tag #	User	Comments
Monitor	DA's Office	CNK7160061	LP2465 Product #: EF224A	HP	64269	Alexandria Loufas	
Monitor	DA's Office	CN-OKHONG-7461-739-9PLB	P2417H	DELL	10003445	Alexandria Loufas	DA Tag# 9TG81J2

Name and title of person completing form: Alexandria Loufas, Paralegal/CRC Restitution Specialist

Phone number: 707-784-6808 Date: 4/3/2019

The following assets must be inventoried:
IT Assets: computer, monitor, fax machine, desktop or network printer, scanner, laptop, copier, etc.
Non-IT Assets: shredder, recorder, TV, any type of furniture – chair, bookcase, cart, credenza, file cabinet, hutch, etc.
Rev. 12/2018

Attachment X

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.

Alexandria Loufas	BOC/Victim Unit	
User Name (Print)	Division or Unit	
	4/3/2019	707-784-6808
User Signature	Date	Phone Number
		707-784-6885
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.

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

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

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

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

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

Attachment XI

CALIFORNIA CalVCB VICTIM COMPENSATION BOARD

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.