Chapter 8 - Support Services

Communications Center

800.1 APPLICABILITY

All personnel.

800.2 PURPOSE AND SCOPE

This policy establishes guidelines for the basic functions of Communications Center and the expectations of professional conduct of all staff who operate within the Communications Center. It addresses the immediate information needs of the Department in the course of its normal daily activities and during emergencies.

800.3 POLICY

It is the policy of the CSUSB University Police Department to provide 24-hour telephone service to the public for information and for routine or emergency assistance. The Department provides two-way radio capability providing continuous communication between Communications Center and department members in the field.

800.4 COMMUNICATIONS CENTER SECURITY

The communications function is vital and central to all emergency service operations. The safety and security of Communications Center, its members and its equipment must be a high priority. Special security procedures should be established in a separate operations manual for Communications Center.

Access to Communications Center shall be limited to Communications Center members, the Watch Commander, command staff and department members with a specific business-related purpose.

800.5 RESPONSIBILITIES

800.5.1 DISPATCH SUPERVISOR

The Chief of Police shall appoint and delegate certain responsibilities to a Dispatch Supervisor. The Dispatch Supervisor is directly responsible to the Operations Lieutenant or the authorized designee.

The responsibilities of the Dispatch Supervisor include, but are not limited to:

(a) Overseeing the efficient and effective operation of Communications Center in coordination with other supervisors.

(b) Scheduling and maintaining dispatcher time records.

(c) Supervising, training and evaluating dispatchers.

(d) Ensuring the radio and telephone recording system is operational.

1. Recordings shall be maintained in accordance with the established records retention schedule and as required by law.

(e) Processing requests for copies of Communications Center information for release.

(f) Maintaining Communications Center database systems.

(g) Maintaining and updating Communications Center procedures manual.

1. Procedures for specific types of crime reports may be necessary. For example, specific questions and instructions may be necessary when talking with a victim of a sexual assault to ensure that his/her health and safety needs are met, as well as steps that he/she may take to preserve evidence.

2. Ensuring dispatcher compliance with established policies and procedures.

(h) Handling internal and external inquiries regarding services provided and accepting personnel complaints in accordance with the Personnel Complaints Policy.

(i) Maintaining a current contact list of State University personnel to be notified in the event of a utility service emergency.

800.5.2 ADDITIONAL PROCEDURES

The Dispatch Supervisor should establish procedures for:

(a) Recording all telephone and radio communications and playback issues.

(b) Storage and retention of recordings.

(c) Security of audio recordings (e.g., passwords, limited access, authorized reviewers, preservation of recordings past normal retention standards).

(d) Availability of current information for dispatchers (e.g., Watch Commander contact, rosters, member tracking methods, member contact, maps, emergency providers, tactical dispatch plans).

(e) Assignment of field members and safety check intervals.

(f) Emergency Medical Dispatch (EMD) instructions.

(g) Procurement of external services (e.g., fire suppression, ambulances, aircraft, tow trucks, taxis).

(h) Protection of essential equipment (e.g., surge protectors, gaseous fire suppression systems, uninterruptible power systems, generators).

(i) Protection of radio transmission lines, antennas and power sources for Communications Center (e.g., security cameras, fences).

(j) Handling misdirected, silent and hang-up calls.

(k) Handling private security alarms, if applicable.

(l) Radio interoperability issues.

800.5.3 DISPATCHERS

Dispatchers report to the Dispatch Supervisor. The responsibilities of the dispatcher include, but are not limited to:

(a) Receiving and handling all incoming and transmitted communications, including:

1. Emergency 9-1-1 lines.
2. Business telephone lines.
3. Telecommunications Device for the Deaf (TDD)/Text Telephone (TTY) equipment.
4. Radio communications with department members in the field and support resources (e.g., fire department, emergency medical services (EMS), allied agency law enforcement units).
5. Other electronic sources of information (e.g., text messages, digital photographs, video).

(b) Documenting the field activities of department members and support resources (e.g., fire department, EMS, allied agency law enforcement units).

(c) Inquiry and entry of information through Communications Center, department and other law enforcement database systems (CLETS, DMV, NCIC).

(d) Monitoring department video surveillance systems.

(e) Maintaining the current status of members in the field, their locations and the nature of calls for service.

(f) Notifying the Watch Commander or field supervisor of emergency activity, including, but not limited to:

(a) Vehicle pursuits.

(b) Foot pursuits.

(c) Assignment of emergency response.

(g) Entering into the Automated Firearms System information about each firearm that has been reported stolen, lost, found, recovered, held for safekeeping, or under observation within seven calendar days of the precipitating event (Penal Code § 11108.2).

800.6 CALL HANDLING

This Department provides members of the public with access to the 9-1-1 system for a single emergency telephone number.

When a call for services is received, the dispatcher will reasonably and quickly attempt to determine whether the call is an emergency or non-emergency, and shall quickly ascertain the call type, location and priority by asking four key questions:

- Where?
- What?

- When?
- Who?

If the dispatcher determines that the caller has a hearing and/or speech impairment or disability, he/she shall immediately initiate a connection with the individual via available TDD/TTY equipment or Telephone Relay Service (TRS), as mandated by the Americans with Disabilities Act (ADA).

If the dispatcher determines that the caller is a limited English proficiency (LEP) individual, the dispatcher should quickly determine whether sufficient information can be obtained to initiate an appropriate response. If language assistance is still needed, the language is known and a language-appropriate authorized interpreter is available in Communications Center, the dispatcher should immediately connect the LEP caller to the authorized interpreter.

If no authorized interpreter is available or the dispatcher is unable to identify the caller's language, the dispatcher will contact the contracted telephonic interpretation service and establish a three-party call connecting the dispatcher, the LEP individual and the interpreter.

Dispatchers should be courteous, patient and respectful when dealing with the public.

800.6.1 EMERGENCY CALLS

A call is considered an emergency when there is an immediate or potential threat to life or serious property damage, and the timely arrival of public safety assistance is of the utmost importance. A person reporting an emergency should not be placed on hold until the dispatcher has obtained all necessary information to ensure the safety of the responding department members and affected individuals.

Emergency calls should be dispatched immediately. The Watch Commander shall be notified of pending emergency calls for service when department members are unavailable for dispatch.

800.6.2 NON-EMERGENCY CALLS

A call is considered a non-emergency call when there is no immediate or potential threat to life or property. A person reporting a non-emergency may be placed on hold, if necessary, to allow the dispatcher to handle a higher priority or emergency call.

The reporting person should be advised if there will be a delay in the dispatcher returning to the telephone line or when there will be a delay in the response for service.

800.7 RADIO COMMUNICATIONS

The police radio system is for official use only, to be used by dispatchers to communicate with department members in the field. All transmissions shall be professional and made in a calm, businesslike manner, using proper language and correct procedures. Such transmissions shall include, but are not limited to:

(a) Members acknowledging the dispatcher with their radio identification call signs and current location.

(b) Dispatchers acknowledging and responding promptly to all radio transmissions.

(c) Members keeping the dispatcher advised of their status and location.

(d) Member and dispatcher acknowledgements shall be concise and without further comment unless additional information is needed.

The Dispatch Supervisor shall be notified of radio procedure violations or other causes for complaint. All complaints and violations will be investigated and reported to the complainant's supervisor and processed through the chain of command.

800.7.1 FEDERAL COMMUNICATIONS COMMISSION COMPLIANCE
CSUSB University Police Department radio operations shall be conducted in accordance with Federal Communications Commission (FCC) procedures and requirements.

800.7.2 RADIO IDENTIFICATION
Radio call signs are assigned to department members based on factors such as duty assignment, uniformed patrol assignment and/or member identification number. Dispatchers shall identify themselves on the radio with the appropriate station name or number, and identify the department member by his/her call sign. Members should use their call signs when initiating communication with the dispatcher. The use of the call sign allows for a brief pause so that the dispatcher can acknowledge the appropriate department member. Members initiating communication with other law enforcement or support agencies shall use their entire radio call sign, which includes the department station name or number.

800.8 DOCUMENTATION

It shall be the responsibility of Communications Center to document all relevant information on calls for service or self-initiated activity. Dispatchers shall attempt to elicit, document and relay as much information as possible to enhance the safety of the member and assist in anticipating conditions that may be encountered at the scene. Desirable information would include, at a minimum:

- Incident control number.
- Date and time of request.
- Name and address of the reporting person, if possible.
- Type of incident reported.
- Involvement of weapons, drugs and/or alcohol.
- Location of incident reported.
- Identification of members assigned as primary and backup.
- Time of dispatch.
- Time of the responding member's arrival.
- Time of member's return to service.
- Disposition or status of reported incident.

800.9 CONFIDENTIALITY

Information that becomes available through Communications Center may be confidential or sensitive in nature. All members of Communications Center shall treat information that becomes known to them as confidential and release that information in accordance with the Protected Information Policy.

Automated data, such as Department of Motor Vehicle records, warrants, criminal history information, records of internal police files or medical information, shall only be made available to authorized law enforcement personnel. Prior to transmitting confidential information via the radio, an admonishment shall be made that confidential information is about to be broadcast.

800.10 TRAINING AND CERTIFICATION

Dispatchers shall receive training consistent with minimum standards established by POST (Penal Code § 13510).

Property and Evidence

801.1 APPLICABILITY
All personnel.

801.2 PURPOSE AND SCOPE
This policy provides for the proper collection, storage, and security of evidence and other property. Additionally, this policy provides for the protection of the chain of evidence and those persons authorized to remove and/or destroy property.

801.3 DEFINITIONS
Property - Includes all items of evidence, items taken for safekeeping and found property.

Evidence - Includes items taken or recovered during an investigation that may be used in the prosecution of a case. This includes photographs and latent fingerprints.

Safekeeping - Includes the following types of property:

- Property obtained by the Department for safekeeping such as a firearm
- Personal property of an arrestee not taken as evidence
- Property taken for safekeeping under authority of a law (e.g., Welfare and Institutions Code § 5150 (mentally ill persons))
- Property held for safekeeping related to a medical aid or similar incident.

Found property - Includes property found by an employee or citizen that has no apparent evidentiary value and where the owner cannot be readily identified or contacted.

801.4 PROPERTY/EVIDENCE HANDLING
Any employee who first comes into possession of any property shall retain such item in his/ her possession until it is properly tagged and placed in the designated evidence locker or storage room. Care and proper packaging shall be taken to maintain the chain of custody for all items.

Where ownership can be established to property with no apparent evidentiary value and items are lawful for the owner to possess, such property may be released to the owner without the need for booking. The property release form must be completed to document the release of property not booked and the owner shall sign the form acknowledging receipt of the items. Where necessary, items released should be photographed before releasing to the appropriate owner. All property shall be entered into the Records Management System (RMS) within the CASE with a proper disposition.

801.4.1 PROPERTY BOOKING PROCEDURE

All items of property must be booked prior to the employee going off-duty unless otherwise approved by a supervisor. Employees booking evidence shall observe the following guidelines:

(a) Enter the item in to the RMS system describing each item of property separately, listing all serial numbers, owner's name, finder's name, and other identifying information or markings.

(b) Proper handling and packaging methods should be adhered to so as not to deface or damage the value of the property.

(c) Print an evidence/property tag and attach it to each package or envelope in which the property is stored.

(d) Place the case number in the upper right corner of the bag, envelope, tag or item.

(e) Personnel entering property or evidence into the RMS system shall ensure their name and identification number are included in the entry module for each item entered, along with a standard disposition date based on the case.

(f) When the item is too large to be placed in a locker, the item may be retained in the designated alternative location with the proper bar code, and the location and the storage location noted on the property within the RMS Case.

801.4.2 NARCOTICS AND DANGEROUS DRUGS

All narcotics and dangerous drugs shall be booked separately using a separate property record. Paraphernalia as defined by Health and Safety Code § 11364 shall also be booked separately. During circumstances where items of paraphernalia are unsafe for processing, such as broken glass, the item may be photographed for evidence and submitted for destruction.

The officer seizing the narcotics and dangerous drugs shall place them in the designated locker. If a 'Request for Analysis' is required, the proper documentation will be submitted by personnel to the Property Officer (or designee) to be submitted to the Crime Lab.

801.4.3 EXPLOSIVES

Officers who encounter a suspected explosive device shall promptly notify their immediate supervisor or the Watch Commander. The bomb squad will be called to handle explosive-related incidents and will be responsible for the handling, storage, sampling and disposal of all suspected explosives.

Explosives will not be retained in the police facility. Only fireworks that are considered stable and safe and road flares or similar signaling devices may be booked into property. All such items shall be stored in proper containers and in an area designated for the storage of flammable materials. The Property Officer is responsible for transporting to the Fire Department, on a regular basis, any fireworks or signaling devices that are not retained as evidence.

801.4.4 EXCEPTIONAL HANDLING

Certain evidence items require a separate process. The following items shall be processed in the described manner:

(a) Bodily fluids such as blood or semen stains shall be air dried prior to booking.

(b) License plates found not to be stolen or connected with a known crime, should be released directly to the Property Officer, or placed in the designated container for return to the Department of Motor Vehicles. No formal property booking process is required.

(c) All bicycles and bicycle frames require a property record. Property bar code tags will be securely attached to each bicycle or bicycle frame. The item may be released directly to the Property Officer, or placed in the bicycle storage area until a Property Officer can log the property.

(d) All cash shall be counted in the presence of a supervisor and the envelope initialed by the booking officer and the supervisor. The Watch Commander shall be contacted for cash believed to be in excess of $1,000 for special handling procedures.

State University property, unless connected to a known criminal case, should be released directly to the appropriate State University department. No formal booking is required. In cases where no responsible person can be located, the property should be booked for safekeeping in the normal manner.

801.4.5 RELINQUISHED FIREARMS

Individuals who relinquish firearms pursuant to the provisions of Penal Code § 29850 shall be issued a receipt that describes the firearm, the serial number or other identification of the firearm at the time of relinquishment (Penal Code § 29810).

Relinquished firearms shall be retained for 30 days, after which time they may be destroyed, retained, sold or otherwise transferred, unless (Penal Code § 29810):

(a) A certificate is issued by a judge of a court of record or the District Attorney stating the firearms shall be retained; or

(b) The convicted person provides written notice of an intent to appeal the conviction that necessitated the relinquishment; or

(c) The Automated Firearms System indicates that the firearm was reported lost or stolen.

1. In such event, the firearm shall be restored to the lawful owner as soon as it is no longer needed as evidence, the lawful owner has identified the weapon and provided proof of ownership, and the Department has complied with the requirements of Penal Code § 33850 et seq.

The firearm shall be entered into the Automated Firearms System, as well as e-Trace System (ATF) to meet the Crime Gun requirements as set forth by the Department of Justice. The Property Officer shall ensure the supervisor is notified of the relinquished firearm for purposes of updating any Automated Firearms System and the disposition of the firearm for purposes of notifying the California Department of Justice (DOJ) (See the Records Section Policy).

801.5 PACKAGING OF PROPERTY

Certain items require special consideration and shall be booked separately as follows:

(a) Narcotics and dangerous drugs

(b) Firearms (ensure they are unloaded and booked separately from ammunition)

(c) Property or evidence with more than one known owner

(d) Paraphernalia as described in Health and Safety Code § 11364

(e) Fireworks

(f) Contraband

801.5.1 PACKAGING CONTAINER

Employees shall package all evidence, except narcotics and dangerous drugs in a suitable container available for its size. Knife boxes should be used to package knives, and syringe tubes should be used to package syringes and needles.

A property bar code tag shall be securely attached to the outside of all items or group of items packaged together.

801.5.2 PACKAGING NARCOTICS

The officer seizing narcotics and dangerous drugs shall retain such evidence in his/her possession until it is properly weighed, packaged, tagged, and placed in the designated evidence locker. Prior to packaging and if the quantity allows, a presumptive test should be made on all suspected narcotics. If conducted, the results of this test shall be included in the officer's report.

Narcotics and dangerous drugs shall be packaged in the appropriate size narcotics envelope available in the report room. The booking officer shall initial the sealed envelope and the evidence tape covering any seal. Narcotics and dangerous drugs shall not be packaged with other items.

A bar code shall be attached to the outside of the container.

801.6 RECORDING OF PROPERTY

The Property Officer receiving custody of evidence or property shall record his/her signature, the date and time the property was received and where the property will be stored within the Records Management System.

A property number shall be obtained for each item or group of items. This number shall be recorded on the property tag and in the Records Management System.

Any changes in the location of property held by the CSUSB University Police Department shall be noted in the Records Management System’s case management section.

801.7 PROPERTY CONTROL

Each time the Property Officer receives property or releases property to another person, he/she shall enter this information in the Records Management System. Officers desiring evidence for

court shall contact the Property Officer at least one business day prior to the court appearance, or date established by the District Attorney's Office.

801.7.1 RESPONSIBILITY OF OTHER PERSONNEL

When property or evidence is received or released, an appropriate entry into the Records Management System shall be completed to maintain the chain of evidence. No evidence is to be released without first receiving written authorization from a supervisor, detective, case officer or authorized designee.

Request for analysis for items other than narcotics or drugs shall be completed on the appropriate forms and submitted to the Property Officer. This request should be completed and submitted without delay, upon booking of the property or evidence.

801.7.2 TRANSFER OF EVIDENCE TO CRIME LABORATORY

The transporting employee will check the evidence out of property, indicating the date and time in the Records Management System and completing the appropriate request for Laboratory Analysis Form.

The Property Officer releasing the evidence must complete the required information in the Records Management System. All applicable forms will be transported with the property to the Crime Lab. Upon delivering the item involved, the officer will record the delivery date and time. The original copy of the analysis form will remain with the evidence and the copy will be returned to the Property Officer for scanning and filing with the case and within the RMS.

801.7.3 STATUS OF EVIDENCE

Each person receiving property will make the appropriate entry to document the chain of evidence. Temporary release of evidence to officers for investigative purposes, or for court, shall be entered wthin the CASE of the RMS Solution, documenting the date, time and to whom released.

The Property Officer shall obtain legal identification and the signature of the person to whom property or evidence is released, including the reason for release. Any employee receiving property or evidence shall be responsible for such property until it is properly returned to property or properly released to another authorized person or entity.

The return of the property or evidence should be recorded in the Records Management System, indicating date, time, and the person who returned the property.

801.7.4 AUTHORITY TO RELEASE PROPERTY AND EVIDENCE

The Associate Director of Police Services or authorized designee shall approve the disposition or destruction of all evidence. Property coming into the care and custody of the Department as lost and found, or safekeeping, etc., should be returned to the owner(s) if ownership can be established. The employee shall document this information on the Notice to Claim Property Form in accordance with department policy and procedure and have the owner sign for said property.

801.7.5 RELEASE OF PROPERTY

All reasonable attempts shall be made to identify the rightful owner of found property or evidence not needed for an investigation.

Release of property or evidence shall be made upon completion of an Authorized Release Form, listing the name and address of the person to whom the item is to be released. The release authorization shall be signed by the authorized supervisor or designee. The property must conform to the items listed within RMS and must specify the specific item(s) being released. Release of all property or evidence shall be documented, reviewed and maintained by scanning corresponding documents into the Records Management System (RMS). For quality control purposes, all property release forms are to be placed in the records bin for verification of accuracy and quality control review of the proper disposition entry into the RMS system.

With the exception of firearms and other property specifically regulated by statute, found property and property held for safekeeping shall be held for a minimum of 90 days. During such period, property personnel shall attempt to contact the rightful owner by telephone and/or mail when sufficient identifying information is available. Property or evidence not held for any other purpose and not claimed within 90 days after receipt (if notification is not feasible); or after notification may be auctioned, donated or destroyed. If such property or evidence is not sold at auction or otherwise lawfully claimed, it may thereafter be destroyed (Civil Code § 2080.6). The final disposition of all such item shall be fully documented within the CASE of the RMS system.

A Property Officer or designee shall release the property or evidence upon proper identification being presented by the owner for which an authorized release has been received. A signature of the person receiving the item shall be recorded on the original release form. After release of the item(s) listed on the Property Release Form the disposition shall be entered into the RMS system and the form scanned into the CASE within RMS. The original form will be placed in the Records Division bin for review.

Under no circumstances shall any firearm be returned to any individual unless and until such person presents valid identification and written notification from the California Department of Justice that conforms to the provisions of Penal Code § 33865.

The Property and Evidence Officer or Supervisor should also make reasonable efforts to determine whether the person is the subject of any court order preventing the person from possessing a firearm and if so, the firearm should not be released to the person while the order is in effect.

This would include any/all restraining orders and/or Armed and Prohibited Persons (APPS) as defined or located in the APPS system of CA-DOJ CLETS systems.

The Department is not required to retain any firearm or other deadly weapon longer than 180 days after notice has been provided to the owner that such firearm or other deadly weapon is available for return. At the expiration of such period, the firearm or other deadly weapon may be processed for disposal in accordance with applicable law (Penal Code § 33875).

801.7.6 DISPUTED CLAIMS TO PROPERTY OR EVIDENCE

Occasionally more than one party may claim an interest in property or evidence being held by the Department, and the legal rights of the parties cannot be clearly established. Such item shall not be released until one party has obtained a valid court order or other undisputed right to the involved property.

All parties should be advised that their claims are civil and in extreme situations, legal counsel for the Department may wish to file an interpleader to resolve the disputed claim (Code of Civil Procedure § 386(b)).

801.7.7 CONTROL OF NARCOTICS AND DANGEROUS DRUGS

The Property and Evidence Officer or designee will be responsible for the storage, control and destruction of all narcotics and dangerous drugs coming into the custody of this department, including paraphernalia as described in Health and Safety Code § 11364.

801.7.8 RELEASE OF FIREARM IN DOMESTIC VIOLENCE MATTERS

Within five days of the expiration of a restraining order issued in a domestic violence matter that required the relinquishment of a firearm, the Property Officer or designee shall return the weapon to the owner if the requirements of Penal Code § 33850 and Penal Code § 33855 are met unless the firearm is determined to be stolen, evidence in a criminal investigation or the individual is otherwise prohibited from possessing a firearm (Family Code § 6389(g); Penal Code § 33855).

801.7.9 RELEASE OF FIREARMS AND WEAPONS IN MENTAL ILLNESS MATTERS

Firearms and other deadly weapons confiscated from an individual detained for an evaluation by a mental health professional or subject to the provisions of Welfare and Institutions Code § 8100 or Welfare and Institutions Code § 8103 shall be released or disposed of as follows:

(a) If a petition for a hearing regarding the return of the weapon has been initiated pursuant to Welfare and Institutions Code § 8102(c), the weapon shall be released or disposed of as provided by an order of the court. If the court orders a firearm returned, the firearm shall not be returned unless and until the person presents valid identification and written notification from the California Department of Justice (DOJ) which conforms to the provisions of Penal Code § 33865.

(b) If no petition has been initiated pursuant to Welfare and Institutions Code § 8102(c) and the weapon is not retained as evidence, the Department shall make the weapon available for return. No firearm will be returned unless and until the person presents valid identification and written notification from the California DOJ which conforms to the provisions of Penal Code § 33865.

(c) Unless the person contacts the Department to facilitate the sale or transfer of the firearm to a licensed dealer pursuant to Penal Code § 33870, firearms not returned should be sold, transferred, destroyed or retained as provided in Welfare and Institutions Code § 8102.

801.7.10 RELEASE OF FIREARMS IN GUN VIOLENCE RESTRAINING ORDER MATTERS
Firearms and ammunition that were taken into temporary custody or surrendered pursuant to a gun violence restraining order shall be returned to the restrained person upon the expiration of the order and in accordance with the requirements of Penal Code § 33850 et seq. (Penal Code § 18120).

If the restrained person who owns the firearms or ammunition does not wish to have the firearm or ammunition returned, he/she is entitled to sell or transfer title to a licensed dealer, provided that the firearms or ammunition are legal to own or possess and the restrained person has right to title of the firearms or ammunition (Penal Code § 18120).

If a person other than the restrained person claims title to the firearms or ammunition surrendered pursuant to Penal Code § 18120 and the CSUSB University Police Department determines him/her to be the lawful owner, the firearms or ammunition shall be returned in accordance with the requirements of Penal Code § 33850 et seq. (Penal Code § 18120).

Firearms and ammunition that are not claimed are subject to the requirements of Penal Code § 34000.

801.8 DISPOSITION OF PROPERTY

All items not to be held for evidence in a pending criminal investigation or proceeding and held for 90 days or longer; in situations where the owner has not been located or fails to claim the property, may be disposed of in compliance with existing laws upon receipt of proper authorization for disposal. The Property Officer shall request a disposition or status on all property which has been held for more than 90 days, and for which no disposition has been received from a supervisor, detective or case agent. At a minimum, two department members shall be involved in the processing of property and evidence being disposed. When this process is completed, both members shall verify the items were accounted for and properly disposed of by signing the appropriate documents or reconciliation report.

801.8.1 EXCEPTIONAL DISPOSITIONS
The following types of evidence shall be destroyed or disposed of in the manner, and at the time prescribed by law, unless a different disposition is ordered by a court of competent jurisdiction:

- Weapons declared by law to be nuisances (Penal Code § 29300; Penal Code § 18010; Penal Code § 32750)
- Animals, birds, and related equipment that have been ordered forfeited by the court (Penal Code § 599a)
- Counterfeiting equipment (Penal Code § 480)
- Gaming devices (Penal Code § 335a)
- Obscene matter ordered to be destroyed by the court (Penal Code § 312)
- Altered vehicles or component parts (Vehicle Code § 10751)
- Narcotics (Health and Safety Code § 11474 et seq.)

- Unclaimed, stolen or embezzled property (Penal Code § 1411)
- Destructive devices (Penal Code § 19000)
- Sexual assault evidence (Penal Code § 680(e))

801.8.2 UNCLAIMED MONEY

If found or seized money is no longer required as evidence and remains unclaimed after three years, the Department shall cause a notice to be published each week for a period of two consecutive weeks in a local newspaper of general circulation (Government Code § 50050). Such notice shall state the amount of money, the fund in which it is held and that the money will become the property of the agency on a designated date not less than 45 days and not more than 60 days after the first publication (Government Code § 50051).

Any individual item with a value of less than $15.00, or any amount if the depositor/owner's name is unknown, which remains unclaimed for a year or by order of the court, may be transferred to the general fund through the Bursar’s Office without the necessity of public notice (Government Code § 50055).

If the money remains unclaimed as of the date designated in the published notice, the money will become the property of this department to fund official law enforcement operations. Money representing restitution collected on behalf of victims shall either be deposited into the Restitution Fund or used for purposes of victim services in accordance to CSUSB policy.

801.8.3 RETENTION OF BIOLOGICAL EVIDENCE

The Property and Evidence Officer or authorized designee shall ensure that no biological evidence held by the Department is destroyed without adequate notification to the following persons, when applicable:

(a) The defendant

(b) The defendant’s attorney

(c) The appropriate prosecutor and Attorney General

(d) Any sexual assault victim

(e) The Investigation Division supervisor

Biological evidence shall be retained for either a minimum period that has been established by law (Penal Code § 1417.9) or that has been established by the Property Officer, or until the expiration of any imposed sentence that is related to the evidence, whichever time period is greater. Following the retention period, notifications should be made by certified mail and should inform the recipient that the evidence will be destroyed after a date specified in the notice unless a motion seeking an order to retain the sample is filed and served on the Department within 180 days of the date of the notification. A record of all certified mail receipts shall be retained in the appropriate file. Any objection to, or motion regarding, the destruction of the biological evidence should be retained in the appropriate file and a copy forwarded to the Investigation Division supervisor.

Biological evidence related to a homicide shall be retained indefinitely and may only be destroyed with the written approval of the Chief of Police and the head of the applicable prosecutor's office.

Biological evidence or other crime scene evidence from an unsolved sexual assault should not be disposed of prior to expiration of the statute of limitations and shall be retained as required in Penal Code § 680. Even after expiration of an applicable statute of limitations, the Investigation Division supervisor should be consulted and the sexual assault victim shall be notified at least 60 days prior to the disposal (Penal Code § 680). Reasons for not analyzing biological evidence shall be documented in writing (Penal Code § 680.3).

801.9 INSPECTIONS OF THE PROPERTY AND EVIDENCE ROOM

(a) Two annual inspections of the evidence storage facilities and practices shall be conducted to ensure adherence to appropriate policies and procedures.

(b) Unannounced inspections of evidence storage areas shall be conducted annually as directed by the Chief of Police.

(c) An annual audit of evidence held by the Department shall be conducted by the Associate Director of Police Services.

(d) Whenever a change is made in personnel who have access to the evidence room, an inventory of all evidence/property shall be made by an individual not associated to the property room or function to ensure that records are correct and all evidence and property is accounted for.

Records Section

802.1 APPLICABILITY

All personnel.

802.2 PURPOSE AND SCOPE

This policy establishes the guidelines for the operational functions of the CSUSB University Police Department Records Section. The policy addresses department file access and internal requests for case reports.

802.3 POLICY

It is the policy of the CSUSB University Police Department to maintain department records securely, professionally, and efficiently.

802.4 RESPONSIBILITIES

802.4.1 RECORDS SUPERVISOR

The Chief of Police shall appoint and delegate records responsibilities to the Associate Director of Police Services. The Associate Director of Police Services shall be directly responsible to the Lieutenant. The Records Supervisor reports to the Associate Director of Police Services.

The responsibilities of the Records Supervisor include, but are not limited to:

(a) Overseeing the efficient and effective operation of the Records Section.

(b) Scheduling and maintaining Records Section time records.

(c) Supervising, training and evaluating Records Section staff.

(d) Maintaining and updating a Records Section procedure manual.

(e) Ensuring compliance with established policies and procedures.

(f) Supervising the access, use and release of protected information (see the Protected Information Policy).

(g) Establishing security and access protocols for case reports designated as sensitive, where additional restrictions to access have been implemented. Sensitive reports may include, but are not limited to:

1. Homicides.
2. Cases involving department members or public officials.
3. Any case where restricted access is prudent.

802.4.2 RECORDS SECTION

The responsibilities of the Records Section include but are not limited to:

(a) Maintaining a records management system for case reports.

(a) The records management system should include a process for numbering, identifying, tracking, and retrieving case reports.

(b) Entering case report information into the records management system.

1. Modification of case reports shall only be made when authorized by a supervisor.

(c) Providing members of the Department with access to case reports when needed for investigation or court proceedings.

(d) Maintaining compliance with federal, state, and local regulations regarding reporting requirements of crime statistics. This includes reporting statistical data to the California Department of Justice (DOJ) for:

1. All officer-involved shootings and incidents involving use of force resulting in serious bodily injury (Government Code § 12525.2).

2. Suspected hate crimes (Penal Code § 13023).

3. Complaints of racial bias against officers (Penal Code § 13012; Penal Code § 13020).

4. Civilian complaints made against officers (Penal Code § 832.5; Penal Code § 13012).

5. Stop data required by Government Code § 12525.5 and 11 CCR 999.226.

(a) The reported information must not contain personally identifiable information of the person stopped or other information exempt from disclosure pursuant to Government Code § 12525.5 (11 CCR 999.228).

(e) Maintaining compliance with federal, state, and local regulations regarding criminal history reports and auditing.

(f) Identifying missing case reports and notifying the responsible member's supervisor.

(g) Updating the Automated Firearms System to reflect any firearms relinquished to the Department and the subsequent disposition to the DOJ pursuant to Penal Code § 34010 (Penal Code § 29810).

(h) Maintaining compliance with the state and DOJ reporting requirements regarding the number of transfers of individuals to immigration authorities and offenses that allowed for the transfers (Government Code § 7284.6(c)(2)).

802.4.3 RECORDS SECTION PROCEDURE MANUAL
The Records Supervisor should establish procedures that address:

(a) Identifying by name persons in reports.

(b) Classifying reports by type of incident or crime.

(c) Tracking reports through the approval process.

(d) Assigning alpha-numerical records to all arrest records.

(e) Managing a warrant and wanted persons file.

802.5 DETERMINATION OF FACTUAL INNOCENCE

In any case where a person has been arrested by officers of the CSUSB University Police Department and no accusatory pleading has been filed, the person arrested may petition the Department to destroy the related arrest records. Petitions should be forwarded to the Administration Supervisor. The Administration Supervisor should promptly contact the prosecuting attorney and request a written opinion as to whether the petitioner is factually innocent of the charges (Penal Code § 851.8). Factual innocence means the accused person did not commit the crime.

Upon receipt of a written opinion from the prosecuting attorney affirming factual innocence, the Administration Supervisor should forward the petition to the Detective Supervisor and the General Counsel for review. After such review and consultation with the General Counsel, the Detective Supervisor and the Administration Supervisor shall decide whether a finding of factual innocence is appropriate.

Upon determination that a finding of factual innocence is appropriate, the Administration Supervisor shall ensure that the arrest record and petition are sealed for later destruction and the required notifications are made to the California DOJ and other law enforcement agencies (Penal Code § 851.8).

The Administration Supervisor should respond to a petition with the Department's decision within 45 days of receipt. Responses should include only the decision of the Department, not an explanation of the analysis leading to the decision.

802.6 ARREST WITHOUT FILING OF ACCUSATORY PLEADING

The Operations Lieutenant should ensure a process is in place for when an individual is arrested and released and no accusatory pleading is filed so that the following occurs (Penal Code § 849.5; Penal Code § 851.6):

(a) The individual is issued a certificate describing the action as a detention.

(b) All references to an arrest are deleted from the arrest records of the Department and the record reflects only a detention.

(c) The California DOJ is notified.

802.7 FILE ACCESS AND SECURITY

The security of files in the Records Section must be a high priority and shall be maintained as mandated by state or federal law. All case reports including but not limited to initial, supplemental, follow-up, evidence, and any other reports related to a police department case, including field interview (FI) cards, criminal history records, and publicly accessible logs, shall be maintained in a secure area within the Records Section, accessible only by authorized members of the Records Section. Access to case reports or files when Records Section staff is not available may be obtained through the Watch Commander.

The Records Section will also maintain a secure file for case reports deemed by the Chief of Police as sensitive or otherwise requiring extraordinary access restrictions.

802.8 ORIGINAL CASE REPORTS

Generally, original case reports shall not be removed from the Records Section. Should an original case report be needed for any reason, the requesting department member shall first obtain authorization from the Records Supervisor. All original case reports removed from the Records Section shall be recorded on a designated report check-out log, which shall be the only authorized manner by which an original case report may be removed from the Records Section.

All original case reports to be removed from the Records Section shall be photocopied and the photocopy retained in the file location of the original case report until the original is returned to the Records Section. The photocopied report shall be shredded upon return of the original report to the file.

802.9 CONFIDENTIALITY

Records Section staff has access to information that may be confidential or sensitive in nature. Records Section staff shall not access, view, or distribute, or allow anyone else to access, view, or distribute any record, file, or report, whether in hard copy or electronic file format, or any other confidential, protected, or sensitive information except in accordance with the Records Maintenance and Release and Protected Information policies and the Records Section procedure manual.

Restoration of Firearm Serial Numbers

803.1 APPLICABILITY
All personnel.

803.2 PURPOSE AND SCOPE
The primary purpose for restoring firearm serial numbers is to determine the prior owners or origin of the item from which the number has been recovered. Thus, property can be returned to rightful owners or investigations can be initiated to curb illegal trade of contraband firearms. The purpose of this plan is to develop standards, methodologies, and safety protocols for the recovery of obliterated serial numbers from firearms and other objects using procedures that are accepted as industry standards in the forensic community. All personnel who are involved in the restoration of serial numbers will observe the following guidelines. This policy complies with Penal Code § 11108.9.

803.3 PROCEDURE
Any firearm coming into the possession of the CSUSB University Police Department as evidence, found property, etc., where the serial numbers have been removed or obliterated will be processed in the following manner:

803.3.1 PRELIMINARY FIREARM EXAMINATION

(a) Always keep the muzzle pointed in a safe direction. Be sure the firearm is in an unloaded condition. This includes removal of the ammunition source (e.g., the detachable magazine, contents of the tubular magazine) as well as the chamber contents.

(b) If the firearm is corroded shut or in a condition that would preclude inspection of the chamber contents, treat the firearm as if it is loaded. Make immediate arrangements for a firearms examiner or other qualified examiner to render the firearm safe.

(c) Accurately record/document the condition of the gun when received. Note the positions of the various components such as the safeties, cylinder, magazine, slide, hammer, etc. Accurately record/document cylinder chamber and magazine contents. Package the ammunition separately.

(d) If the firearm is to be processed for fingerprints or trace evidence, process before the serial number restoration is attempted. First record/document important aspects such as halos on the revolver cylinder face or other relevant evidence that might be obscured by the fingerprinting chemicals.

803.3.2 PROPERTY BOOKING PROCEDURE

Any employee taking possession of a firearm with removed/obliterated serial numbers shall book the firearm into property following standard procedures. The employee booking the firearm shall indicate on the property form that serial numbers have been removed or obliterated.

803.3.3 OFFICER RESPONSIBILITY

The Property Officer receiving a firearm when the serial numbers have been removed or obliterated shall arrange for the firearm to be transported to the crime lab for restoration and maintain the chain of evidence.

803.3.4 DOCUMENTATION

Case reports are prepared in order to document the chain of custody and the initial examination and handling of evidence from the time it is received/collected until it is released.

This report must include a record of the manner in which and/or from whom the firearm was received. This may appear on the request form or property form depending on the type of evidence.

803.3.5 FIREARM TRACE

After the serial number has been restored (or partially restored) by the criminalistics laboratory, the Property Officer will complete a Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) National Tracing Center (NTC) Obliterated Serial Number Trace Request Form (ATF 3312.1-OBL) and forward the form to the NTC in Falling Waters, West Virginia or enter the data into the ATF eTrace system.

803.4 BULLET AND CASING IDENTIFICATION

Exemplar bullets and cartridge cases from the firearm, depending upon acceptance criteria and protocol, may be submitted to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) National Integrated Ballistic Information Network (NIBIN) which uses the Integrated Ballistic Identification System (IBIS) technology to search the national database and compare with ballistic evidence recovered from other crime scenes.

Records Maintenance and Release

804.1 APPLICABILITY
All personnel.

804.2 PURPOSE AND SCOPE
This policy provides guidance on the maintenance and release of department records. Protected information is separately covered in the Protected Information Policy.

804.3 POLICY
The CSUSB University Police Department is committed to providing public access to records in a manner that is consistent with the California Public Records Act (Government Code § 6250 et seq.).

804.4 CUSTODIAN OF RECORDS RESPONSIBILITIES
The Chief of Police shall designate a Custodian of Records. The responsibilities of the Custodian of Records include but are not limited to:

(a) Managing the records management system for the Department, including the retention, archiving, release, and destruction of department public records.

(b) Maintaining and updating the department records retention schedule including:

1. Identifying the minimum length of time the Department must keep records.

2. Identifying the department division responsible for the original record.

(c) Establishing rules regarding the inspection and copying of department public records as reasonably necessary for the protection of such records.

(d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of records.

(f) Ensuring a current schedule of fees for public records as allowed by law is available (Government Code § 6253).

(g) Determining how the department's website may be used to post public records in accordance with Government Code § 6253.

(h) Ensuring that public records posted on the Department website meet the requirements of Government Code § 6253.10 including but not limited to posting in an open format where a record may be retrieved, downloaded, indexed, and searched by a commonly used internet search application.

(i) Ensuring that a list and description, when applicable, of enterprise systems (as defined by Government Code § 6270.5) is publicly available upon request and posted in a prominent location on the Department’s website.

804.5 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any department member who receives a request for any record shall route the request to the Custodian of Records or the authorized designee.

804.5.1 REQUESTS FOR RECORDS

Any member of the public, including the media and elected officials, may access unrestricted records of this department, during regular business hours by submitting a written and signed request that reasonably describes each record sought and paying any associated fees (Government Code § 6253).

The processing of requests for any record is subject to the following (Government Code § 6253):

(a) The Department is not required to create records that do not exist.

(b) Victims of an incident or their authorized representative shall not be required to show proof of legal presence in the United States to obtain department records or information. If identification is required, a current driver's license or identification card issued by any state in the United States, a current passport issued by the United States or a foreign government with which the United States has a diplomatic relationship or current Matricula Consular card is acceptable (Government Code § 6254.30).

(c) Either the requested record or the reason for non-disclosure will be provided promptly, but no later than 10 days from the date of request, unless unusual circumstances preclude doing so. If more time is needed, an extension of up to 14 additional days may be authorized by the Custodian of Records or the authorized designee. If an extension is authorized, the Department shall provide the requester written notice that includes the reason for the extension and the anticipated date of the response.

1. When the request does not reasonably describe the records sought, the Custodian of Records shall assist the requester in making the request focused and effective in a way to identify the records or information that would be responsive to the request including providing assistance for overcoming any practical basis for denying access to the records or information. The Custodian of Records shall also assist in describing the information technology and physical location in which the record exists (Government Code § 6253.1).

2. If the record requested is available on the department website, the requester may be directed to the location on the website where the record is posted. If the requester is unable to access or reproduce the record, a copy of the record shall be promptly provided.

(d) Upon request, a record shall be provided in an electronic format utilized by the Department. Records shall not be provided only in electronic format unless specifically requested (Government Code § 6253.9).

(e) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released.

1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for

the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the department-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.

(f) If a record request is denied in whole or part, the requester shall be provided a written response that includes the statutory exemption for withholding the record or facts that the public interest served by nondisclosure outweighs the interest served by disclosure (Government Code § 6255). The written response shall also include the names, titles or positions of each person responsible for the denial.

804.6 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address, and telephone number; and medical or disability information that is contained in any driver license record, motor vehicle record, or any department record, including traffic collision reports, are restricted except as authorized by the Department, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

(b) Social Security numbers (Government Code § 6254.29).

(c) Personnel records, medical records, and similar records which would involve an unwarranted invasion of personal privacy except as allowed by law (Government Code § 6254; Penal Code § 832.7; Penal Code § 832.8; Evidence Code § 1043 et seq.).

1. Peace officer personnel records that are deemed confidential shall not be made public or otherwise released to unauthorized individuals or entities absent a valid court order.

2. The identity of any officer subject to any criminal or administrative investigation shall not be released without the consent of the involved officer, prior approval of the Chief of Police, or as required by law.

(d) Victim information that may be protected by statutes, including victims of certain crimes who have requested that their identifying information be kept confidential, victims who are minors, and victims of certain offenses (e.g., sex crimes or human trafficking, Penal Code § 293). Addresses and telephone numbers of a victim or a witness to any arrested person or to any person who may be a defendant in a criminal action shall not be disclosed, unless it is required by law (Government Code § 6254; Penal Code § 841.5).

1. Victims of certain offenses (e.g., domestic violence, sexual assault, stalking, human trafficking, adult abuse) or their representatives shall be provided, upon request and without charge, one copy of all incident report face sheets, one copy of all incident reports, or both, pursuant to the requirements and time frames of Family Code § 6228.

2. Victims of sexual assault, upon written request, shall be provided a free copy of the initial crime report regardless of whether the report has been closed. Personal identifying information may be redacted (Penal Code § 680.2(b)).

(e) Video or audio recordings created during the commission or investigation of the crime of rape, incest, sexual assault, domestic violence, or child abuse that depicts the face, intimate body part, or voice of a victim of the incident except as provided by Government Code § 6254.4.5.

(f) Information involving confidential informants, intelligence information, information that would endanger the safety of any person involved, or information that would endanger the successful completion of the investigation or a related investigation. This includes analysis and conclusions of investigating officers (Evidence Code § 1041; Government Code § 6254).

1. Absent a statutory exemption to the contrary or other lawful reason to deem information from reports confidential, information from unrestricted agency reports shall be made public as outlined in Government Code § 6254(f).

(g) Local criminal history information including but not limited to arrest history and disposition, and fingerprints shall only be subject to release to those agencies and individuals set forth in Penal Code § 13300.

1. All requests from criminal defendants and their authorized representatives (including attorneys) shall be referred to the District Attorney, General Counsel, or the courts pursuant to Penal Code § 1054.5.

(h) Certain types of reports involving but not limited to child abuse and molestation (Penal Code § 11167.5), elder and dependent abuse (Welfare and Institutions Code § 15633), and juveniles (Welfare and Institutions Code § 827).

(i) Sealed autopsy and private medical information concerning a murdered child with the exceptions that allow dissemination of those reports to law enforcement agents, prosecutors, defendants, or civil litigants under state and federal discovery laws (Code of Civil Procedure §130).

(j) Information contained in applications for licenses to carry firearms or other files that indicates when or where the applicant is vulnerable or which contains medical or psychological information (Government Code § 6254).

(k) Traffic collision reports (and related supplemental reports) shall be considered confidential and subject to release only to the California Highway Patrol, Department of Motor Vehicles (DMV), other law enforcement agencies, and those individuals and their authorized representatives set forth in Vehicle Code § 20012.

(l) Any record created exclusively in anticipation of potential litigation involving this department (Government Code § 6254).

(m) Any memorandum from legal counsel until the pending litigation has been adjudicated or otherwise settled (Government Code § 6254.25).

(n) Records relating to the security of the department’s electronic technology systems (Government Code § 6254.19).

(o) A record of a civilian complaint, or the investigations, findings, or dispositions of that complaint if the complaint is frivolous, as defined by Code of Civil Procedure § 128.5, or if the complaint is unfounded (Penal Code § 832.7 (b)(8)).

(p) Any other record not addressed in this policy shall not be subject to release where such record is exempt or prohibited from disclosure pursuant to state or federal law, including but not limited to provisions of the Evidence Code relating to privilege (Government Code § 6254).

(q) Information connected with juvenile court proceedings or the detention or custody of a juvenile. Federal officials may be required to obtain a court order to obtain certain juvenile information (Welfare and Institutions Code § 827.9; Welfare and Institutions Code § 831).

804.7 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the District Attorney, General Counsel or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Department so that a timely response can be prepared.

804.8 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the department name and to whom the record was released.

Each audio/video recording released should include the department name and to whom the record was released.

804.9 SEALED RECORD ORDERS

Sealed record orders received by the Department shall be reviewed for appropriate action by the Custodian of Records. The Custodian of Records shall seal such records as ordered by the court. Records may include but are not limited to a record of arrest, investigation, detention, or conviction. Once the record is sealed, members shall respond to any inquiry as though the record did not exist (Penal Code § 851.8; Welfare and Institutions Code § 781).

When an arrest record is sealed pursuant to Penal Code § 851.87, Penal Code § 851.90, Penal Code § 851.91, Penal Code § 1000.4, or Penal Code § 1001.9, the Records Supervisor shall ensure that the required notations on local summary criminal history information and police

investigative reports are made. Sealed records may be disclosed or used as authorized by Penal Code § 851.92.

804.10 SECURITY BREACHES

The Records Supervisor shall ensure notice is given anytime there is a reasonable belief an unauthorized person has acquired either unencrypted personal identifying information or encrypted personal information along with the encryption key or security credential stored in any Department information system (Civil Code § 1798.29).

Notice shall be given as soon as reasonably practicable to all individuals whose information may have been acquired. The notification may be delayed if the Department determines that notification will impede a criminal investigation or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

For the purposes of this requirement, personal identifying information includes an individual's first name or first initial and last name in combination with any one or more of the following:

- Social Security number
- Driver license number or California identification card number
- Account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
- Medical information
- Health insurance information
- A username or email address, in combination with a password or security question and answer that permits access to an online account
- Information or data collected by Automated License Plate Reader (ALPR) technology

804.10.1 FORM OF NOTICE

(a) The notice shall be written in plain language, be consistent with the format provided in Civil Code § 1798.29 and include, to the extent possible, the following:

1. The date of the notice.
2. Name and contact information for the CSUSB University Police Department.
3. A list of the types of personal information that were or are reasonably believed to have been acquired.
4. The estimated date or date range within which the security breach occurred.
5. Whether the notification was delayed as a result of a law enforcement investigation.
6. A general description of the security breach.

7. The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a Social Security number or a driver license or California identification card number.

(b) The notice may also include information about what the CSUSB University Police Department has done to protect individuals whose information has been breached and may include information on steps that the person whose information has been breached may take to protect him/herself (Civil Code § 1798.29).

(c) When a breach involves an online account, and only a username or email address in combination with either a password or security question and answer that would permit access to an online account, and no other personal information has been breached (Civil Code § 1798.29):

1. Notification may be provided electronically or in another form directing the person to promptly change either his/her password or security question and answer, as applicable, or to take other appropriate steps to protect the online account with the Department in addition to any other online accounts for which the person uses the same username or email address and password or security question and answer.

2. When the breach involves an email address that was furnished by the CSUSB University Police Department, notification of the breach should not be sent to that email address but should instead be made by another appropriate medium as prescribed by Civil Code § 1798.29.

804.10.2 MANNER OF NOTICE

(a) Notice may be provided by one of the following methods (Civil Code § 1798.29):

1. Written notice.

2. Electronic notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC § 7001.

3. Substitute notice if the cost of providing notice would exceed $250,000, the number of individuals exceeds 500,000 or the Department does not have sufficient contact information. Substitute notice shall consist of all of the following:

(a) Email notice when the Department has an email address for the subject person.

(b) Conspicuous posting of the notice on the department's webpage for a minimum of 30 days.

4. Notification to major statewide media and the California Information Security Office within the California Department of Technology.

(b) If a single breach requires the Department to notify more than 500 California residents, the Department shall electronically submit a sample copy of the notification, excluding any personally identifiable information, to the Attorney General.

Protected Information

805.1 APPLICABILITY

All perosnnel.

805.2 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the CSUSB University Police Department. This policy addresses the protected information that is used in the day-to-day operation of the Department and not the public records information covered in the Records Maintenance and Release Policy.

805.2.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the CSUSB University Police Department and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

805.3 POLICY

Members of the CSUSB University Police Department will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

805.4 RESPONSIBILITIES

The Chief of Police shall select a member of the Department to coordinate the use of protected information.

The responsibilities of this position include, but are not limited to:

(a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicle (DMV) records and California Law Enforcement Telecommunications System (CLETS).

(b) Developing, disseminating and maintaining procedures that adopt or comply with the U.S. Department of Justice’s current Criminal Justice Information Services (CJIS) Security Policy.

(c) Developing, disseminating and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release and security of protected information.

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

805.5 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, CSUSB University Police Department policy or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution.

805.5.1 PENALTIES FOR MISUSE OF RECORDS

It is a misdemeanor to furnish, buy, receive or possess Department of Justice criminal history information without authorization by law (Penal Code § 11143).

Authorized persons or agencies violating state regulations regarding the security of Criminal Offender Record Information (CORI) maintained by the California Department of Justice may lose direct access to CORI (11 CCR 702).

805.6 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Division to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other police department members or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

805.6.1 REVIEW OF CRIMINAL OFFENDER RECORD
Individuals requesting to review their own California criminal history information shall be referred to the Department of Justice (Penal Code § 11121).

Individuals shall be allowed to review their arrest or conviction record on file with the Department after complying with all legal requirements regarding authority and procedures in Penal Code § 11120 through Penal Code § 11127 (Penal Code § 13321).

805.7 SECURITY OF PROTECTED INFORMATION

The Chief of Police will select a member of the Department to oversee the security of protected information.

The responsibilities of this position include, but are not limited to:

(a) Developing and maintaining security practices, procedures and training.

(b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.

(c) Establishing procedures to provide for the preparation, prevention, detection, analysis and containment of security incidents including computer attacks.

(d) Tracking, documenting and reporting all breach of security incidents to the Chief of Police and appropriate authorities.

805.7.1 MEMBER RESPONSIBILITIES
Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

805.8 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

805.9 CALIFORNIA RELIGIOUS FREEDOM ACT

Members shall not release personal information from any agency database for the purpose of investigation or enforcement of any program compiling data on individuals based on religious belief, practice, affiliation, national origin or ethnicity (Government Code § 8310.3).

Computers and Digital Evidence

806.1 APPLICABILITY

All personnel.

806.2 PURPOSE AND SCOPE

This policy establishes procedures for the seizure and storage of computers, personal communications devices (PCDs) digital cameras, digital recorders and other electronic devices that are capable of storing digital information; and for the preservation and storage of digital evidence. All evidence seized and/or processed pursuant to this policy shall be done so in compliance with clearly established Fourth Amendment and search and seizure provisions.

806.3 SEIZING COMPUTERS AND RELATED EVIDENCE

Computer equipment requires specialized training and handling to preserve its value as evidence. Officers should be aware of the potential to destroy information through careless or improper handling, and utilize the most knowledgeable available resources. When seizing a computer and accessories the following steps should be taken:

(a) Photograph each item, front and back, specifically including cable connections to other items. Look for a phone line or cable to a modem for Internet access.

(b) Do not overlook the possibility of the presence of physical evidence on and around the hardware relevant to the particular investigation such as fingerprints, biological or trace evidence, and/or documents.

(c) If the computer is off, do not turn it on.

(d) If the computer is on, do not shut it down normally and do not click on anything or examine any files.

1. Photograph the screen, if possible, and note any programs or windows that appear to be open and running.
2. Disconnect the power cable from the back of the computer box or if a portable notebook style, disconnect any power cable from the case and remove the battery).

(e) Label each item with case number, evidence sheet number, and item number.

(f) Handle and transport the computer and storage media (e.g., tape, discs, memory cards, flash memory, external drives) with care so that potential evidence is not lost.

(g) Lodge all computer items in the Property Room. Do not store computers where normal room temperature and humidity is not maintained.

(h) At minimum, officers should document the following in related reports:

1. Where the computer was located and whether or not it was in operation.

2. Who was using it at the time.
3. Who claimed ownership.
4. If it can be determined, how it was being used.

(i) In most cases when a computer is involved in criminal acts and is in the possession of the suspect, the computer itself and all storage devices (hard drives, tape drives, and disk drives) should be seized along with all media. Accessories (printers, monitors, mouse, scanner, keyboard, cables, software and manuals) should not be seized unless as a precursor to forfeiture.

806.3.1 BUSINESS OR NETWORKED COMPUTERS

If the computer belongs to a business or is part of a network, it may not be feasible to seize the entire computer. Cases involving networks require specialized handling. Officers should contact a certified forensic computer examiner for instructions or a response to the scene. It may be possible to perform an on-site inspection, or to image the hard drive only of the involved computer. This should only be done by someone specifically trained in processing computers for evidence.

806.3.2 FORENSIC EXAMINATION OF COMPUTERS

If an examination of the contents of the computer's hard drive, or floppy disks, compact discs, or any other storage media is required, forward the following items to a computer forensic examiner:

(a) Copy of report(s) involving the computer, including the Evidence/Property sheet.

(b) Copy of a consent to search form signed by the computer owner or the person in possession of the computer, or a copy of a search warrant authorizing the search of the computer hard drive for evidence relating to investigation.

(c) A listing of the items to search for (e.g., photographs, financial records, e-mail, documents).

(d) An exact duplicate of the hard drive or disk will be made using a forensic computer and a forensic software program by someone trained in the examination of computer storage devices for evidence.

806.4 SEIZING DIGITAL STORAGE MEDIA

Digital storage media including hard drives, floppy discs, CD's, DVD's, tapes, memory cards, or flash memory devices should be seized and stored in a manner that will protect them from damage.

(a) If the media has a write-protection tab or switch, it should be activated.

(b) Do not review, access or open digital files prior to submission. If the information is needed for immediate investigation request the Property and Evidence Officer to copy the contents to an appropriate form of storage media.

(c) Many kinds of storage media can be erased or damaged by magnetic fields. Keep all media away from magnetic devices, electric motors, radio transmitters or other sources of magnetic fields.

(d) Do not leave storage media where they would be subject to excessive heat such as in a parked vehicle on a hot day.

(e) Use plastic cases designed to protect the media, or other protective packaging, to prevent damage.

806.5 SEIZING PCDS

Personal communication devices such as cell phones, PDAs or other hand-held devices connected to any communication network must be handled with care to preserve evidence that may be on the device including messages, stored data and/or images.

(a) Officers should not attempt to access, review or search the contents of such devices prior to examination by a forensic expert. Unsent messages can be lost, data can be inadvertently deleted and incoming messages can override stored messages.

(b) Do not turn the device on or off. The device should be placed in a solid metal container such as a paint can or in a faraday bag, to prevent the device from sending or receiving information from its host network.

(c) When seizing the devices, also seize the charging units and keep them plugged in to the chargers until they can be examined. If the batteries go dead all the data may be lost.

806.6 DIGITAL EVIDENCE RECORDED BY OFFICERS

Officers handling and submitting recorded and digitally stored evidence from digital cameras and audio or video recorders will comply with these procedures to ensure the integrity and admissibility of such evidence.

806.6.1 COLLECTION OF DIGITAL EVIDENCE

Once evidence is recorded it shall not be erased, deleted or altered in any way prior to submission. All photographs taken will be preserved regardless of quality, composition or relevance. Video and audio files will not be altered in any way.

806.6.2 SUBMISSION OF DIGITAL MEDIA

The following are required procedures for the submission of digital media used by cameras or other recorders:

(a) The recording media (smart card, compact flash card or any other media) shall be submitted into evidence.

(b) As soon as possible following the collection of evidence, the camera operator is to remove the memory card from their digital camera and place the card into a plastic carrier. The card and carrier are then to be placed into a zip-lock type baggie. The

camera operator shall write their name and the related case number on the outside of the baggie before placing in the film drop box along with the evidence form.

(c) Evidence technicians will make a copy of the memory card using appropriate storage media. Once they have verified that the images properly transferred to the storage media, the technicians will erase the memory card for re-use. The storage media will be marked as the original.

(d) Officers requiring a copy of the digital files must request a copy on the evidence form when submitted to evidence.

806.6.3 DOWNLOADING OF DIGITAL FILES

Digital information such as video or audio files recorded on devices using internal memory must be downloaded to storage media. The following procedures are to be followed:

(a) Files should not be opened or reviewed prior to downloading and storage.

(b) Where possible, the device should be connected to a computer and the files accessed directly from the computer directory or downloaded to a folder on the host computer for copying to the storage media.

806.6.4 PRESERVATION OF DIGITAL EVIDENCE

(a) Only evidence technicians are authorized to copy original digital media that is held as evidence. The original digital media shall remain in evidence and shall remain unaltered.

(b) Digital images that are enhanced to provide a better quality photograph for identification and investigative purposes must only be made from a copy of the original media.

(c) If any enhancement is done to the copy of the original, it shall be noted in the corresponding incident report.

Jeanne Clery Campus Security Act

807.1 APPLICABILITY

All personnel.

807.2 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines to ensure this department fulfills its obligation in complying with the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act) as well as applicable California Education Code requirements.

807.3 POLICY AND CLERY COMPLIANCE TEAM

The CSUSB University Police Department encourages accurate and prompt reporting of all crimes and takes all such reports seriously (20 USC § 1092(f)(1)(C)(iii)). Reports will be accepted in any manner, including in person or in writing, at any CSUSB University Police Department facility. Reports will be accepted anonymously, by phone or via email or on the institution's website.

It is the policy of the CSUSB University Police Department to comply with the Clery Act. Compliance with the Clery Act requires a joint effort between the CSUSB University Police Department and the administration of the institution. To that end, the University has developed a Clery Compliance Team that works to ensure campus-wide coordination and participation. The CCT includes components responsible for executive oversight, review and resources related to the University's Clery program.

Supervisors assigned areas of responsibility in the following policy sections are expected to be familiar with the subsections of 20 USC § 1092(f) and 34 CFR 668.46 that are relevant to their responsibilities.

807.4 POLICY, PROCEDURE AND PROGRAM DEVELOPMENT

The Chief of Police will, with the assistance of the Clery Compliance Team:

(a) Ensure that the CSUSB University Police Department establishes procedures for immediate emergency response and evacuation, including the use of electronic and cellular communication and testing of these procedures (20 USC § 1092(f)(1)(J)(i); 20 USC § 1092(f)(1)(J)(iii)).

(b) Enter into written agreements as appropriate with local law enforcement agencies to (Education Code § 67381.1):

1. Identify roles in the investigation of alleged criminal offenses on campus (20 USC § 1092(f)(1)(C)(ii)).

(a) This includes identification of the responsibilities for sexual assault, hate crimes and Part 1 violent crime investigations (e.g., willful homicide, forcible rape, robbery or aggravated assault as defined in the FBI's Uniform Crime Reporting (UCR) Handbook), and establishing the specific

geographical boundaries of each agency's responsibility, including maps as necessary (Education Code § 67381).

2. Assist in the monitoring and reporting of criminal activity at off-campus student organizations that are recognized by the institution and engaged in by students attending the institution, including student organizations with off-campus housing facilities (20 USC § 1092(f)(1)(G)).

3. Ensure coordination of emergency response and evacuation procedures, including procedures to immediately notify the campus community upon the confirmation of a significant emergency or dangerous situation (20 USC § 1092(f)(1)(J)). At CSUSB the emergency management role is under the office of Risk Management, however these activities are in close coordination with the University Police Department.

4. Notify the CSUSB University Police Department of criminal offenses reported to local law enforcement agencies to assist the institution in meeting its reporting requirements under the Clery Act (20 USC § 1092(f)(1)(F)).

5. Notify the CSUSB University Police Department of criminal offenses reported to local law enforcement agencies to assist in making information available to the campus community in a timely manner and to aid in the prevention of similar crimes. Such disseminated information shall withhold the names of victims as confidential (20 USC § 1092(f)(3)).

(c) Appoint a designee to develop programs that are designed to inform students and employees about campus security procedures and practices, and to encourage students and employees to be responsible for their own security and the security of others (20 USC § 1092(f)(1)(D)).

(d) Appoint a designee to develop programs to inform students and employees about the prevention of crime (20 USC § 1092(f)(1)(E)).

(e) Appoint a designee to develop educational programs to promote the awareness of rape, acquaintance rape, domestic violence, dating violence, sexual assault and stalking, and what to do if an offense occurs, including but not limited to, who should be contacted, the importance of preserving evidence and to whom the alleged offense should be reported (20 USC § 1092(f)(8)(B)). The designee shall also develop written materials to be distributed to reporting persons that explains the rights and options provided for under 20 USC § 1092 (20 USC § 1092(f)(8)(C)).

(f) Appoint a designee to make the appropriate notifications to institution staff regarding missing person investigations in order to ensure that the institution complies with the requirements of 34 CFR 668.46(h).

All such duties, delegations and appointments will be coordinated with and by the campus administration, and in many cases these activities will be the responsibility of other offices on campus.

807.4.1 ADDITIONAL REQUIREMENTS

The Chief of Police, with the assistance of the Clery Compliance Team: (Education Code § 67386):

(a) Assist the institution with the development of policies and procedures relating to sexual assault, domestic violence, dating violence and stalking involving a student whether it occurred on- or off-campus including:

1. The differences between standards of proof and defenses in criminal investigations and administrative or disciplinary matters.

2. Victim-centered protocols including privacy protection, responses to reports, interviews, investigations, required notifications and participation by victim advocates and other supporting individuals.

(b) Assist, as appropriate, with trauma-informed training for campus personnel involved in investigating and adjudicating sexual assault, domestic violence, dating violence and stalking cases.

(c) Assist, as appropriate, in the development of the institution's comprehensive prevention and outreach programs addressing sexual violence, domestic violence, dating violence, and stalking.

(d) Ensure that any reported Part 1 violent crime, sexual assault or hate crime described in Penal Code § 422.55 (whether it occurred on- or off-campus), is reported as soon as practicable to any local law enforcement agency with investigation responsibilities pursuant to a written agreement with the CSUSB University Police Department or the institution (Education Code § 67380).

1. The identification of the victim shall be withheld, unless the victim consents to being identified after being informed of the right to have his/her personally identifying information withheld. If the victim does not consent to being identified, then the alleged assailant shall not be identified unless the institution determines that the alleged assailant represents a serious or ongoing threat to the safety of the students, employees or the institution, and the immediate assistance of the CSUSB University Police Department is necessary to contact or detain the assailant (Education Code § 67380).

2. If the institution discloses the identity of the alleged assailant to the CSUSB University Police Department, the institution must immediately inform the victim of that disclosure (Education Code § 67380).

All such duties, delegations and appointments will be coordinated with and by the campus administration, and in many cases these activities will be the responsibility of other offices on campus.

807.5 RECORDS COLLECTION AND RETENTION

The Records Supervisor is responsible for maintaining CSUSB University Police Department statistics and making reasonable good-faith efforts to obtain statistics from other law enforcement agencies as necessary to allow the institution to comply with its reporting requirements under the Clery Act (20 USC § 1092(f)(1)(F)). The statistics shall be compiled as follows:

(a) Statistics concerning the occurrence of the following criminal offenses reported to this department or to local police agencies that occurred on campus, in or on non-campus buildings or property, and on public property including streets, sidewalks and parking facilities within the campus or immediately adjacent to and accessible from the campus (20 USC § 1092(f)(1)(F)(i); 34 CFR 668.46(c)):

1. Murder
2. Sex offenses, forcible or non-forcible
3. Robbery
4. Aggravated assault
5. Burglary
6. Motor vehicle theft
7. Manslaughter
8. Arson
9. Arrests or persons referred for campus disciplinary action for liquor law violations, drug-related violations and weapons possession
10. Dating violence, domestic violence and stalking

(b) Statistics concerning the crimes described in the section above, theft, simple assault, intimidation, destruction, damage or vandalism of property, and other crimes involving bodily injury to any person where the victim was intentionally selected because of his/her actual or perceived race, sex, religion, gender, gender identity, sexual orientation, ethnicity or disability. These statistics should be collected and reported according to the category of prejudice (20 USC § 1092(f)(1)(F)(ii); 34 CFR 668.46(c)).

1. The statistics shall be compiled using the definitions in the FBI's UCR system and modifications made pursuant to the Hate Crime Statistics Act (20 USC § 1092(f)(7); 34 CFR 668.46(c)(9)). For the offenses of domestic violence, dating violence and stalking, such statistics shall be compiled in accordance with the definitions used in the Violence Against Women Act (20 USC § 1092(f)(7); 34 USC § 12291; 34 CFR 668.46(a)). The statistics will be categorized separately as offenses that occur in the following places (20 USC § 1092(f)(12); 34 CFR 668.46(c)(5)):
    (a) On campus.
    (b) In or on a non-campus building or property.
    (c) On public property.
    (d) In dormitories or other on-campus, residential or student facilities.

(c) Statistics will be included by the calendar year in which the crime was reported to the CSUSB University Police Department (34 CFR 668.46(c)(3)).

(d) Stalking offenses will include a statistic for each year in which the stalking conduct is reported and will be recorded as occurring either at the first location where the stalking occurred or the location where the victim became aware of the conduct (34 CFR 668.46(c)(6)).

(e) Statistics will include the three most recent calendar years (20 USC § 1092(f)(1)(F); 34 CFR 668.46(c)).

(f) The statistics shall not identify victims of crimes or persons accused of crimes (20 USC § 1092(f)(7)).

807.5.1 CRIME LOG

The Records Supervisor is responsible for ensuring a daily crime log is created and maintained as follows (20 USC § 1092(f)(4); 34 CFR 668.46(f)):

(a) The daily crime log will record all crimes reported to the CSUSB University Police Department, including the nature, date, time and general location of each crime, and the disposition, if known.

(b) All log entries shall be made within two business days of the initial report being made to the Department.

(c) If new information about an entry becomes available, then the new information shall be recorded in the log not later than two business days after the information becomes available to the police department or security department.

(d) The daily crime log for the most recent 60-day period shall be open to the public for inspection at all times during normal business hours. Any portion of the log that is older than 60 days must be made available within two business days of a request for public inspection. Information in the log is not required to be disclosed when:

1. Disclosure of the information is prohibited by law.
2. Disclosure would jeopardize the confidentiality of the victim.
3. There is clear and convincing evidence that the release of such information would jeopardize an ongoing criminal investigation or the safety of an individual, may cause a suspect to flee or evade detection, or could result in the destruction of evidence. In any of these cases, the information may be withheld until that damage is no longer likely to occur from the release of such information.

807.5.2 COMPILING RECORDS FOR DISCLOSURE REQUIREMENTS

The Records Supervisor is also responsible for compiling the following to allow the institution to comply with its disclosure requirements under Education Code § 67380:

(a) All occurrences reported to the CSUSB University Police Department and all arrests for crimes that are committed on campus that involve violence, hate violence, theft, destruction of property, illegal drugs, or alcohol intoxication.

(b) All occurrences of noncriminal acts of hate violence reported to the CSUSB University Police Department for which a written report is prepared.

807.6 INFORMATION DISSEMINATION

It is the responsibility of the Clery Compliance Team to ensure that the required Clery Act disclosures are properly forwarded to campus administration and community members in accordance with institution procedures. This includes:

(a) Procedures for providing emergency notification of crimes or other incidents and evacuations that might represent an imminent threat to the safety of students or employees (20 USC § 1092(f)(3); 34 CFR 668.46(e); 34 CFR 668.46 (g)).

(b) Procedures for notifying the campus community about crimes considered to be a threat to other students and employees in order to aid in the prevention of similar crimes. Such disseminated information shall withhold the names of victims as confidential (20 USC § 1092(f)(3)).

(c) Information necessary for the institution to prepare its annual security report (20 USC § 1092(f)(1); 34 CFR 668.46(b)). This report will include, but is not limited to:

1. Crime statistics and the policies for preparing the crime statistics.
2. Crime and emergency reporting procedures, including the responses to such reports.
3. Policies concerning security of and access to campus facilities.
4. Crime, dating violence, domestic violence, sexual assault and stalking awareness and prevention programs, including
    (a) Procedures victims should follow.
    (b) Procedures for protecting the confidentiality of victims and other necessary parties.
5. Enforcement policies related to alcohol and illegal drugs.
6. Locations where the campus community can obtain information about registered sex offenders.
7. Emergency response and evacuation procedures.
8. Missing student notification procedures.
9. Information addressing the jurisdiction and authority of campus security including any working relationships and agreements between campus security personnel and both state and local law enforcement agencies.

Timely Warning

808.1 POLICY

(a) CSU San Bernardino will send a Timely Warning Notice to the campus community for notification about serious crimes against people that occur on campus when it is determined the incident may pose a serious or ongoing threat to members of the campus community. Timely Warning Notices are usually distributed for the following crime classifications: criminal homicide, sexual assault, sex offenses, aggravated assault, arson, burglary and larceny, hate-related crimes, motor vehicle theft, and robbery. All incidents are considered on a case-by-case basis, depending on the facts, when and where it was reported and occurred, and other pertinent information known by the University Police Department (UPD) at the time of report.

(b) The timely warning will be issued as soon as pertinent information is available.

(c) The issuing of a Timely Warning Notice shall be decided in light of all of the facts surrounding a crime, including factors such as the nature of the crime, the continuing danger to the campus community, and the possible risk of compromising law enforcement efforts. Timely Warning Notices will include information that promotes safety, describes the type of reported crime, and reports the time and location at which the reported crime occurred, and offers specific advice to the campus community regarding steps to take to avoid becoming a victim.

(d) A Timely Warning Notice may be distributed for other crimes as determined necessary by the Chief of Police or designee.

808.2 VICTIM NOTIFICATION

CSU San Bernardino considers the well-being of crime survivors to be a top priority and seeks to maintain a balanced approach in the issuing of a Timely Warning Notice, ensuring compliance with applicable laws while taking into account the needs and concerns of both the victim(s) and the campus community. When reasonably practicable, a crime victim will be notified in advance that a Timely Warning Notice will be issued to the campus community.

808.3 ISSUANCE PROCESS

A consultation group is responsible for issuing a Timely Warning Notice. The consultation group consists of: the Chief of Police or designee, the Public Information Officer when needed, and the Vice President for Administration & Finance or his designee. They shall work in consultation before issuing a Timely Warning Notice. The Vice President for Administration &Finance or his designee shall make a notification to the Office of the President. While efforts are made to confer with the consultation group prior to issuing a timely warning whenever possible, the Chief of Police or designee has authority to issue a Timely Warning Notice without consultation when necessary to ensure the safety of the campus community.

808.4 WARNING METHODS

Timely Warning Notices are issued through a variety of methods, depending on the specific circumstances, and may include:

a. email messages (Colleagues/Students)

b. text messaging to cell phones as part of the ENS system

c. UPD and University Advancement websites

d. public announcements

e. postings and signage in residence halls and other highly visible locations throughout campus

808.5 RECIPIENT RESPONSIBILITIES

Recipients of a Timely Warning Notice are responsible for updating their emergency contact information with the University.

808.6 RELATIONSHIP TO CLERY ACT

The Clery Act and federal regulations require CSU San Bernardino to disclose emergency response and evacuation procedures. A summary of these procedures is included in the University's Annual Security Report (ASR), which can be found on the University Police website. http://police.csusb.edu/index.html

Emergency Notification to Campus

809.1 APPLICABILITY

Sworn and dispatch personnel.

809.2 POLICY

CSUSB will immediately notify the campus community using the Emergency Notification System (ENS) upon confirmation of a significant emergency or dangerous situation involving an immediate threat to the health or safety of students or employees occurring on campus. A significant emergency or dangerous situation is confirmed for the purposes of distributing an emergency notification when Chief of Police or designee receives reports or other evidence from community members, local first responders, the National Weather Service or other similar means that leads one to believe that a significant emergency or dangerous situation exists for the entire campus or a segment of the campus population.

When reasonable a consultation group is responsible for issuing an ENS. The consultation group consists of: the Chief of Police or designee, the Public Information Officer, the Vice President for Administration & Finance or his designee and other stakeholders when needed. They shall work in consultation issuing an ENS if reasonable and possible. The Vice President for Administration &Finance or his designee shall make a notification to the Office of the President. While efforts are made to confer with the consultation group prior to issuing an ENS, the Chief of Police or designee has authority to issue an ENS without consultation when necessary to ensure the safety of the campus community.

Because an emergency notification is time-sensitive, the Chief of Police or designee shall take into account the safety of the campus community, determine what information should be released, and issue an ENS notification based upon the evidence known at the time of issuance. An ENS message will be released as soon as reasonably necessary, and without delay, unless notification will compromise efforts to assist a victim, or to contain, respond to, or otherwise mitigate the emergency.

809.3 SYSTEM DESCRIPTION

The ENS allows notifications to geographical areas of persons or select persons on campus. ENS messages will be sent to all members of the campus community. Messages are sent to select recipients only during testing of the ENS system. CSUSB uses an Emergency Notification System (ENS) to notify students, staff and faculty when it is determined that there is a significant emergency or dangerous situation involving an immediate threat to the health or safety of students or employees on campus. The ENS is used to transmit brief, urgent messages to the campus community as quickly as possible.

809.4 TYPICAL USAGE

The following is a list of situations where one might expect an ENS message:

(a) Earthquake
(b) Gas leak
(c) Terrorist incident
(d) Armed intruder/Active Shooter
(e) Bomb threat
(f) Civil unrest or rioting
(g) Explosion
(h) Approaching extreme weather
(i) Campus closure due to declared civil emergency or infectious disease concerns
(j) Other incident or situation requiring rapid communication of life safety information

809.5 RECIPIENT RESPONSIBILITY

Recipients of ENS messages are responsible for updating their emergency contact information with the University. All members of the University community are encouraged to add their cellular phone number so they may receive ENS messages via text, which is the quickest form of communication.