Station Security and Visitors

208.1 PURPOSE AND SCOPE

> This is an **CRITICAL / MODERATE-RISK** Policy for the Department. Department
> members to whom this policy applies must have a good working knowledge
> of the policy and how to reference it when needed (**YELLOW STRIPE**).

(a) The purpose of this policy is to define the procedures that will be implemented to improve the physical security of Oakley Police Department Facilities. The safety and confidentiality of our members, visitors, volunteers, victims, witnesses, and arrestees is the responsibility of all of our members.

(b) The Department plays host to a variety of confidential communications and situations on a daily basis. Access control is the foundation for maintaining this type of an environment.

(c) The Police Department and our data systems are also a repository of confidential information that can be observed, read, overheard, or deduced. It's the responsibility of all employees of the Department to understand the role they play in making our work areas safe and secure.

(d) It is the intent of the Oakley Police Department to comply with both Federal and State Department of Justice Information Security Requirements.

208.2 POLICY

(a) Access to all Police Department Facilities and work areas will be controlled. These controls have been instituted for the safety and security of the occupants of these facilities and the materials they contain.

(b) The integrity of our investigative process and of our evidentiary chain demands strict access control procedures be implemented and enforced by all employees.

(c) Adherence to security procedures ensure that only authorized persons are allowed access and that all persons entering the employee areas of the building have been properly identified and screened.

208.3 REFERENCES

(a) Criminal Justice Information Services (CJIS) Security Policy, US Department of Justice (US-DOJ), V 5.5, June 2016

(b) CLETS Policies, Practices and Procedures, California Department of Justice (CA-DOJ), September 2014

208.4 RELATED MANUAL SECTION(S)

(a) OPD Manual Section 806, Confidential Information - Access / Destruction

208.5 RESPONSIBILITIES OF ALL PERSONNEL

(a) Station security is everyone's responsibility. Department personnel should challenge any person in the police facility that is not recognized as an employee and is not wearing a visitor's badge. Employees expecting visitors shall notify the Records Unit, who will ensure the visitor is properly processed and escorted to the host employee.

(b) During normal business hours, each unit leader within the Police Department is responsible for the security of their unit areas and the station.

(c) After normal business hours, the On-Duty Supervisor is responsible for the security of the station.

(d) Security issues will be addressed immediately and violations of the security policy reported through the Chain of Command to the Chief of Police.

208.6 BUILDING SECURITY

(a) Entry into the Police Station will be restricted.

(b) All exterior doors to the police building and other police department outbuildings shall remain closed and locked when not in use. The propping open of any door for any length of time is not allowed unless an identified employee monitors the entry/exit of that door.

(c) It shall be the responsibility of every employee to stop, and in a professional manner, question any persons in any police facility, ████████████████████ ████████████████████████████████████. These persons should be immediately escorted to the front desk and required to adhere to this policy.

(d) Any person being subject to a Health and Safety § 11590 or Penal Code § 290 own recognizance booking, or any person brought into the interior of any police department building for the purposes of detention/arrest should be immediately pat searched for weapons, to include any other property the person has in his/her possession prior to any processing.

(e) **Public Areas**

1. Public Areas are those areas that are accessible to the general public without being escorted and without having met any other requirements. These public areas are accessible during normal operating hours specific to that area and are the following:

    (a) Front/Main Parking Lot

    (b) Front Lobby

2. There are no restrictions or escort requirements for these areas.

(f) **Non-Public Areas**

1. Non-Public Areas are areas that are accessible to individuals having permission or authority to enter the Police Station and property beyond those specified in the "public" area definitions. ████████████████████████

███████████████████████████████████████ must be escorted by an authorized employee at all times.

2. Non-Public Areas of the Police Department are designated as the following areas:

   (a) All other non-designated open areas within the building.

   (b) Restrooms

   (c) Locker Rooms

   (d) Report Writing Room

   (e) Line-Up Room

   (f) Employee Lunch/Break Room

   (g) Main Hallways Within The Police Department

   (h) Secured Parking Lot

(g) **Secured Areas**

1. Secured Areas are areas within the Police Department that have limited access. Only those individuals having authority shall have access to specific secured areas. These individuals may have access to certain secured areas and not others, depending upon their level of access authority. Secured areas will be limited access during normal business operating hours. Supervisory personnel and above, or those individuals having the specific authority to access a particular area may access those areas during non-business hours. These secured areas are designated as the following areas:

   (a) Evidence packaging room.

   (b) Evidence Vehicle Storage Yard

   (c) Command Staff Offices

   (d) Chief's Office

(h) **Restricted Areas**

1. Restricted Areas are areas within the Police Department that have restricted access and access is highly controlled, regardless of supervisory status or hours of operation. Only designated individuals having authority from the Chief of Police or his/her designee shall have access to specific restricted areas. Restricted areas are designated as the following areas:

   (a) **Armory**. No employee, except for designated Rangemasters, supervisors and staff shall enter the armory at any time.

   (b) **Records Unit**. Authorized department personnel may retrieve case files in the records area as required for legitimate business. Original case files shall not leave the records area at any time.

   (c) **Server Cage**.

      (d) **Property and Evidence Office and Storage Room**. No employee, except for property officers and authorized, designated staff members, shall enter the secure area of the property room at any time.

      (e) **Prisoner Processing Area** (when occupied).

      (f) **Interview Room** (when occupied).

      (g) ▮▮▮▮▮▮▮▮▮▮▮▮▮▮

208.7 MINIMUM STANDARDS FOR ACCESS

(a) Access to the Oakley Police Department and within the facility is controlled under the authority of the Chief of Police or his/her designee. To ensure high standards of security within the Oakley Police Department, all individuals entering the facility, building(s) and property beyond the Front Lobby must have permission and authority to enter and must adhere to one of the following:

    1. Be a current Police Department employee in good standing.

    2. Escorted by a current/authorized Police Department employee at all times.

    3. Successfully passed a "Less Than Full" background check.

    4. Successfully passed a full background check.

    5. On-duty emergency personnel responding to an actual emergency within the building (i.e., ambulance, or Fire personnel).

(b) Relatives and/or friends, who wish to contact an employee in person, shall come to the front counter and request the receptionist to advise the employee. Friends and/ or relatives of employees must be escorted at all times.

(c) During non-business hours, employees may escort friends and/or relatives through the facility for the purpose of tours, etc. However, they must be monitored and accompanied at all times.

208.8 VISITORS

(a) All visitors to the Police Department shall check-in at the front desk.

(b) The employee to whom the visitor wishes to see shall be notified. The employee to whom the visitor wishes to see will ensure that a visitor's badge is issued to the visitor prior to entering the secure area of the department.

(c) ▮▮

A visitor is any person not employed by the police department. Police employees shall remain with their visitors. If a circumstance arises where an employee must leave their visitor, the visitor shall be escorted to a conference room or lobby where they can comfortably wait for the employee to return. Visitors shall not wait unattended for an employee in a common office, work area, hallway, or lunchroom.

(d) **Volunteers**: As an exception to the visitor policy, explorers or any other department volunteers, shall be issued and wear an identification badge clearly visible on the front

of their clothing while in the police building at all times. Volunteers are not required to wear an identification badge if they are in uniform. Volunteers shall have the same unescorted access to the building as any other employee as outlined in this policy and within the rules and practices of their particular position.

(e) **Family**: As an exception to the visitor policy, any family member of a current Department member may be left unattended in secure areas. Family members shall have a visible visitor badge if left unaccompanied.

(f) **Visitor Log.**

1. A visitor log entry shall be maintained for all visitors. The visitor log shall be kept in the Records Unit. Front desk personnel shall obtain government ID from visitors and compete the visitor log by entering the date of the visit, the time of visitor's arrival and departure, the visiting person's name and ID number, the name of the Department personnel associated (if applicable) with the visitor's meeting, visitor badge number, and the name of the front desk personnel completing the log.

2.
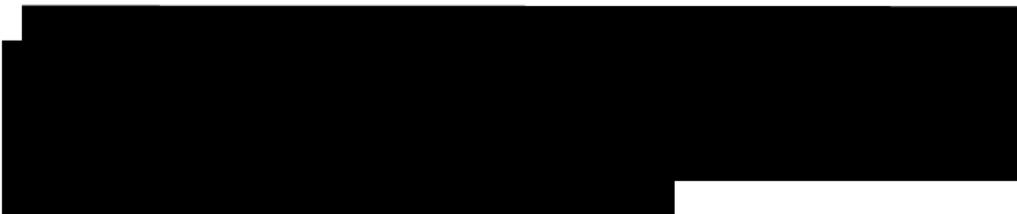
(g) **Visitor Escorts.**

1. Unless a visitor is approved by a supervisor for unescorted access to the station, front desk personnel are to contact the employee sought by the visitor once a visitor's badge has been issued. The employee receiving the visitor shall personally contact the visitor at the front desk and escort the person to his/her office or meeting place. Once the visit has been concluded, the employee shall personally escort the visitor to the front lobby and direct the visitor to return the visitor badge.

(h) **Non-Department Employees**

1. City employees from other Departments shall wear their City ID Card visible at all times. Non-police City employees will be escorted.

2. The following persons are exempt from being required to display a visitor badge:

   (a) The City Manager.

   (b) City Council Members.

   (c) City Employees..

   (d) Visitors of the Chief of Police.

   (e) Escorted family members of Department personnel.

   (f) Members of a group on a station tour guided by a Department employee.

(g) Arrestees, detainees, and other persons while in custody, either confined in a secure detention area or under continuous escort by an officer.

(h) Janitorial personnel.

(i) Any other group, with the approval of the On-Duty Supervisor which by its size would make formal check–in procedures unfeasible.

208.9 CONTRACT SERVICE PROVIDERS

(a) All contract service providers working in the Police Department are required to obtain a visitor's badge. The Department employee who summoned the contract service should then be contacted to meet and escort the contract employee. The Department employee will be responsible for providing reasonable oversight of all activities while in the facility.

(b) Technicians/repair persons who respond to the facility after hours shall be under the supervision of the On-Duty Supervisor.

208.10 OUTSIDE LAW ENFORCEMENT PERSONNEL

(a) Visiting law enforcement personnel must display a badge or ID card in plain view in lieu of a visitor's badge. No recordation is necessary in the visitor's log. If visiting law enforcement personnel are unable to display an ID card or a badge, a visitor's badge should be issued.

208.11 INTERVIEW ROOM USE

(a) The interview rooms are available for use by any police officer or agency to perform an interview.

(b) An OPD Staff Member will be assigned to assisted any allied agencies while using the rooms.

(c) Police personnel are to utilize these rooms for official uses only.

208.12 BUILDING ACCESS CARDS / FOBS / CODES

[REDACTED]

208.13 PARKING LOT ACCESS

(a) All department employees will be provided the code for the police department parking lot.

(b) The gate code will be changed:

1. When the code has been compromised.

2. When an employee is terminated.

3. At least annually.

(c) Officers shall lock their patrol cars and roll up all windows whenever parked in the police parking lot for any length of time.

(d) **Automated Gate Openers.**

1. The Police Department Parking Lot may be accessed through the use of an automatic opener.

2. Individuals who have been issued openers are responsible for the security of the device.

3. Individuals who lose or misplace their openers will report the missing device to the Administrative Services Sergeant.

208.14 BUILDING KEYS

(a) Some employees will be issued keys to various doors in the Police Department.

(b) Individuals who have been issued keys are responsible for maintaining control of their assigned keys.

(c) Individuals who lose or misplace their assigned keys will report their loss immediately to the Administrative Services Sergeant.

(d)   Employees who will no longer need an assigned key due to transfers shall turn in their keys to the Administrative Services Sergeant.

(e)   Employees are prohibited from exchanging keys with other employees without the direct involvement of the Administrative Services Sergeant.

208.15   BUILDING DOOR SECURITY

(a)   Employees should not leave facility perimeter doors propped open. If propping open a door is necessary for maintenance or other temporary needs, the door shall be attended at all times. Any employee who finds a facility perimeter door propped open and unattended is required to close the door and ensure that it is secure. The Administrative Services Sergeant should be notified of any malfunctioning door.

208.16   STATION INSPECTION AND MAINTENANCE

(a)   All Shift Supervisors shall perform a basic inspection of the station at least once during their shift. The inspection should include the report writing room, locker rooms, processing area, and line-up room.

(b)   The Day Shift Supervisor is responsible for inspecting the facility's outer perimeter and parking areas during their shifts. The focus of the inspection should be risk management and facility security issues including:

1.   Hazards.

2.   Security.

3.   Display of offensive materials.

4.   Overall appearance and cleanliness.

5.   Doors and gates secured.

6.   Suspicious packages or persons.

7.   Security of vehicles.

(c)   Employees should also be alert to risk management issues and shall report any concerns to a supervisor.

208.17   SURVEILLANCE CAMERA SYSTEM

Station Security and Visitors

208.18   DELIVERIES TO THE FRONT DESK

(a)   During weekday business hours, front desk personnel should receive all package deliveries.

(b)   After hour deliveries should be received and left in the Records Unit for delivery to the addressee on the next business day.

208.19   PERSONAL DELIVERIES

(a)   Personal deliveries of packages to the Police Department may be made on an infrequent basis.

(b)   Employees will not have their mail delivered to the Police Department,

208.20   STATION TOURS

(a)   The Oakley Police Department recognizes the value and importance of conducting tours of the Police Department to acquaint members of the community with the functions and operation of the Department.

(b)   **Requests for Station Tours**

1.   The Records Unit shall coordinate tours of the police facility. An employee shall be assigned to provide the tour and is responsible for ensuring adequate supervision of the group to avoid accidental injuries or visitors wandering from the group.

(c)   **Permissible Areas for Tours**

1.   The following areas may be entered by tour groups:

(a)   Processing Area (when unoccupied).

(b)   Parking Lot.

(c)   Detective Unit Area.

(d)   Traffic Unit Area.

(e)   Line-Up Room (when not in use).

(f)   Sergeant's Office (when not in use)

(g)   A patrol car demonstration of the emergency lights, siren, and equipment may be provided. The shotgun shall not be removed from the locking mechanism.

(d)   **Impermissible Areas for Tours**

1.   Tour groups shall not enter any secure portion of the facility, such as:

(a)   Locker Rooms.

(b)   Interview Rooms.

(c)   Assigned offices.

(d)   Patrol Armory.

(e)   Evidence Room.

208.21   OFF-SITE LOCATION SECURITY

(a)   **Off-Site Evidence Vehicle Storage Yard.** The Police Evidence Vehicle Storage Yard is located off site in a secure and alarmed location. Only authorized sworn and professional staff field personnel are allowed entrance to this site. Police personnel must log all entries to this facility.

208.22   SECURITY AWARENESS TRAINING (DOJ CJIS 5.2)

(a)   The Records Manager is responsible for managing CJIS Security Awareness Training and maintaining those records. CJIS Security Awareness Training is typically incorporated in the routine CA CLETS Access User Program.

(b)   Employee and volunteers who work in the Police Facility are required to completed Security Awareness Training within six months of initial assignment and biennially thereafter.

(c)   IT Personnel are required to complete Security Awareness Training, which is accomplished through the CA CLETS On-Line System.

(d)   Certificates of CJIS training from other police agencies may be accepted; however, local training will also be provided.

(e)   The OPD Records Manager is responsible for maintaining these training records.

(f)   **Level One Security Awareness Training (DOJ CJIS 5.2.1.1)**

  1.   As a minimum, all employees/volunteers with unescorted access to areas containing CJI will receive training on the following topics:

   (a)   Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

   (b)   Incident response (Identify points of contact and individual actions).

   (c)   Implications of noncompliance.

   (d)   Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.

(g)   **Level Two Security Awareness Training (DOJ CJIS 5.2.1.2)**

  1.   All OPD Personnel will complete Level 2 Security Awareness Training. In addition to the information covered in Section 208.21.1, the following material will be trained:

   (a)   Dissemination and destruction.

   (b)   Social engineering.

   (c)   Threats, vulnerabilities, and risks associated with handling of CJI.

   (d)   Proper handling and marking of CJI.

    (e)   Protect information subject to confidentiality concerns — hardcopy through destruction.

    (f)   Media protection.

(h)   **Level Three Security Awareness Training (DOJ CJIS 5.2.1.3)**

    1.   All OPD personnel will complete Level 3 Security Awareness Training. In addition to the information contained in Section 208.21.1 and 208.21.2, the training will include:

    (a)   Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

    (b)   Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.

    (c)   Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.

    (d)   Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.

    (e)   Individual accountability—explain what this means in the agency.

    (f)   Access control issues—address least privilege and separation of duties.

    (g)   Personally owned equipment and software—state whether allowed or not (e.g., copyrights).

    (h)   Laptop security—address both physical and information security issues.

    (i)   Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.

    (j)   Handheld device security issues—address both physical and wireless security issues.

    (k)   Physical Security—increases in risks to systems and data.

    (l)   Spam.

    (m)   Web usage—allowed versus prohibited; monitoring of user activity.

    (n)   Unknown e-mail/attachments.

    (o)   Protection from viruses, worms, Trojan horses, and other malicious code.

    (p)   Password usage and management—including creation, frequency of changes, and protection.

    (q)   Rules that describe responsibilities and expected behavior with regard to information system usage.

(i)   **Level Four Security Awareness Training (DOJ CJIS 5.2.1.4)**

1.   All OPD IT Personnel will complete mandatory Level 1,2, and 3 training along with the following topics:

    (a)   Network infrastructure protection measures.

    (b)   Access control measures.

    (c)   Timely application of system patches—part of configuration management.

    (d)   Data backup and storage—centralized or decentralized approach.

    (e)   Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.

208.23 REVISION DATE

    (a)   27 AUG 19