OC SAN ORANGE COUNTY SANITATION DISTRICT	SOP-208 (Ver. 3) Workplace Security
Standard Operating Procedure (SOP)	Effective: 1/25/2022 Supersedes: 11/02/2020
Approved By: James D. Herberg General Manager James Herberg	

I. Purpose

The purpose of the Workplace Security Policy is to establish, implement, and enforce comprehensive security polices which support a secure working environment for all OC San employees and contractors through proactive security measures, communication, and teamwork.

Risk Management is dedicated to protecting all employees, contractors, and critical infrastructure against acts of violence which would cause injury or harm and disrupt OC San's ability to provide effective wastewater collection and treatment and protect the public health.

II. Definitions

Access: The ability and opportunity to gain entry to a protected area.

Access Control: The control of persons, vehicles, and materials through entrances and exits of a protected area; an aspect of security that often utilizes hardware systems and specialized procedures to control and monitor movements into, out of, or within a protected area. Access to various areas may be limited to place or time, or a combination of both. Some access control systems feature historical data bases for reference.

Access Control Card Reader: Access control card readers are used in physical security systems to read a credential that allows access through access control points such as a locked door or a gate.

Badge: A device or token indicating membership in a group such as an employee identification card, access control card, or the shield worn by public safety personnel or security officers.

Card Key: A plastic card that contains coded information capable of being read by access control card readers placed at the entry and exit points of the protected facility.

Closed Circuit Television (CCTV): A television installation in which the signal is transmitted to a defined number of receivers.

Contract Security: Protective services provided by one company, specializing in such services, to another company on a paid, contractual basis.

Civil Demonstration: A civil protest/disturbance that takes form an organized public demonstration of disapproval with particular action, idea, or incident.

Integrated Emergency Response Plan (IERP): A collection of Emergency Operational Plans (EOPs) within OC San.

Lighting: In the context of physical security, lighting which aids in the protection of assets, particularly as it relates to the prevention and early detection of unwanted intrusion. In an industrial facility, security lighting is required for protection of property, to discourage trespassers, and to provide a means for security to identify personnel.

Physical Security: Infrastructure designed prevent harm, damage, or unauthorized access to employees, contractors, and critical infrastructure.

Protected Area: An area protected by physical security safeguards and access controls.

Protected Process Area (PPA): An area within the perimeter of the plant(s) and pump stations that require additional physical protection because of their critical nature to plant operations. Access to PPA by contractors, consultants, vendors, and suppliers require OC San responsible parties' approval and supervision prior to and when entering.

Security Committee: The Security Committee is comprised of fourteen (14) members who serve in a leadership and/or supervisory role throughout OC San. The purpose of the Committee is to provide a formal means for employees to effectively participate with management in the identification and resolution of security concerns, and to promote the safety and security of OC San. Risk Management staff and the Committee will work in conjunction to safeguard physical and cyber resources, identify conditions or circumstances that may pose risks to the safety and security of the facilities, and prepare OC San to effectively respond to emergencies.

Security Plan: Plan used to assist OC San in improving the safety and security of its facilities, employees, and the public. The Plan offers an effective security approach for water support facilities includes equipment and systems to deter, detect, delay, and respond to a threat prior to the disruptive risk achieving its objective.

Security Threat: Anything that has the potential to cause serious harm to people or infrastructure and will disrupt OC San's ability to provide effective wastewater treatment.

Vital Operation Area (VOA): Located within the protected process area and requires additional security measures. Additional authorization is required for unescorted access to vital operation areas.

Vulnerability: A vulnerability is a weakness or lapse in infrastructure which can be exploited by a hostile actor who wishes to inflict harm to people or property.

Workplace: Any location, either permanent or temporary, where an employee performs any work-related duty. This includes, but is not limited to, administrative buildings, surrounding perimeters, parking lots, off site locations, and the travel between work locations.

Workplace Security: Workplace security includes threats, violent behavior, harassment, intimidation, and other disruptive behavior, direct, indirect, implied, or actual from any person, and directed toward any person, occurring either at an OC San facility or in connection with the conduct of OC San business without regard to location.

III. Responsibilities

A. Risk Management:

1. Write and implement security policy for OC San employees. Risk Management will serve as a conduit and provide information on physical security, risk mitigation, infrastructure resiliency, and emergency response issue.

2. Investigate and report security incidents and follow-up as necessary to improve security performance. Risk Management will share lessons learned from such incidents using after-action reports (AAR), correspondence, and other tools to take corrective action(s), prevent future occurrences, and impalement best practices.

3. Administer outside security services such as professional consulting services, guard services, and investigative services as they relate to security

4. Conduct security and emergency preparedness exercises.

5. Administer and control the identification card and access control program.

6. Provide guidance in the implementation of physical controls and barriers of OC San facilities.

7. Provide liaison with local, state, and federal law enforcement and emergency management agencies if applicable.

8. Administer employee, contractor, and visitor access to OC San facilities.

9. Administer vehicular access and parking control at all OC San facilities.

10. Maintain and update the Security and Emergency Management SharePoint page.

B. Security Committee

1. Responsible for supporting and fostering a safe and secure environment in all facilities owned and/or operated by OC San. Promotes an appropriate level of security on OC San facilities and safeguards OC San property and physical assets.

2. Provides observations, input, and recommendations on strategic security and emergency response issues.

3. Review findings and corrective actions of reported security incidents.

4. Provide Committee updates to their department employees.

5. Review and recommend current and future security procedures and projects.

6. Ensure that security measures will be considered at the earliest stage of new projects, such as the expansion of plant critical infrastructure.

C. Management and Supervision

1. Individuals in supervisory and management roles are responsible for ensuring that employees under their supervision are aware of security policies and procedures for the reporting of security problems, accidents, emergencies, crimes, and threats. They are also responsible for ensuring that emergency preparedness and continuity of operations plans are followed and communicated to all employees to ensure familiarity with, and coordination between departments and emergency responders. Evaluate the performance of all employees in complying with OC San workplace security measures.

2. Follow progressive discipline for employees who fail to comply with workplace security practices.

3. Recognize employees who perform work practices which promote security in the workplace.

4. Managers and Supervisors ensure that appropriate physical-security measures are taken to mitigate the loss of equipment and supplies. Physical protective measures include barriers, lighting, and electronic security systems, and access control. Supervisors shall always enforce all access control policies ensuring doors are secure. Doors propped open for the purpose of routine work or delivers should be monitored while work is in progress.

5. The preservation of OC San assets is the responsibility of every employee. This responsibility includes taking appropriate measures to prevent losses due to willful actions which would result in personal injury, property damage (i.e., vandalism) or theft. First line supervisors and managers have the additional responsibility of facilitating the gathering of reports of losses, which will be forwarded to Risk Management for tabulation or additional investigation.

6. Managers and Supervisors have the responsibility of promoting a secure working environment. Managers and Supervisors have increased responsibility of ensuring that employees are adhering to all security policies and procedures outlined in this SOP.

D. Employees

1. All employees are responsible for the safety and the security of our workplace. Employees must follow all security and traffic signs, abide by and aid in the enforcement of all security policies and procedures, and assist in maintaining a safe and secure working environment.

2. Security and safety rules apply to all OC San employees, visitors, and contractors. Violators of these rules can be subject to disciplinary action up to and including termination. For contracted consultants who violate OC San security policy they can be subject to contract termination or removal from the site.

3. Abide by all posted security and traffic control signs and security personnel.

4. OC San assets are to be protected and to be used for authorized purposes only.

5. Employees must comply with Workplace Security Policy which safeguards OC San assets against theft, damage, and unauthorized use.

6. All employees must work with Risk Management to ensure best physical security practices are being enforced.

7. All employees are responsible for submitting visitor information into the Visitor Registration system located at https://visitors/.

8. All employees have the responsibility for reporting all known or suspected asset losses that come to their attention to their immediate supervisor. First line supervisors and managers are responsible for ensuring that OC San Security/Loss Reports are completed for asset loss with their area of responsibility. This reporting must be completed in five (5) business days and be accurate. Security/Loss Reports provide the basis for an accurate tracking of security risk exposures. The tracking will serve to facilitate analysis, identify weaknesses in current business processes, and provide for corrective actions to minimize future losses.

9. If you discovered a crime has been committed or witness a crime in progress, please report it to your immediate supervisor, Risk Management, and the local police department. If the crime is in progress dial 2222 or 911 if located off site. Additionally, you should notify the Control or Operations Center of the crime. If safe, remain on site or at the location to assist management and Risk Management personnel in the reporting of the crime. In cases where an employee is the victim of a crime, such as vandalism or theft, the employee should be available to report incident to police and/or security.

10. Employees shall complete a security loss/incident report form and property disposition form which is available on the San Box (intranet site). First line supervisors and managers are responsible for ensuring a copy of the completed incident report is provided to Risk Management.

IV. Physical Security Plan

A. The Physical Security Plan outlines and offers consistent direction for the security standards of both new construction builds and existing building retrofits. Data was primarily utilized from the American Society of Civil Engineers (ASCE), “Guidelines for the Physical Security of Wastewater/Stormwater Utilities” publication. This Plan includes the following:

   1. Conduct a site risk assessment during the early phases of the site design, by utilizing a customized OC San Risk Assessment scorecard.

   2. Determine the risk-level of a specific OC San site (low-risk, medium-risk, high-risk).

   3. Recommend physical security components for various types of risk-level sites (CCTV coverage, physical barriers, lighting standards, alarm systems, etc.)

   4. Provide detailed and consistent descriptions and features of the various physical security components for operators, engineers, and OC San executives

B. The Physical Security Plan is located on the Risk Management SharePoint under the Security page. The plan shall be utilized to guide Risk Management and all other stakeholders in the implementation of physical security infrastructure.

V. Vulnerability and Risk Assessments

A. Risk Management is responsible for conducting vulnerability and risk assessments for OC San owned critical infrastructure at Plant 1, Plant 2, and all offsite facilities in accordance with the Physical Security Plan. Assessments consist of the identification of workplace security threats and hazards and potential solutions or mitigation measures. OC San utilizes mitigation strategies and best practices to mitigate risk and reduce threats.

B. Assess the need for video surveillance systems, security lighting, hardening infrastructure, and access control mechanisms.

C. Assess procedures for reporting suspicious persons or activities.

D. Assess entry control points (ECP) and visitor access policies and procedures.

VI. Security Incidents in the Workplace

A. OC San promotes a safe work environment for all employees and contractors. The safe work environment includes an environment that is free from violence, threats of violence, harassment, intimidation, and other disruptive behavior.

B. All workplace violence issues, incidents, and procedures will be reported in accordance with Human Resources (HR) Policy 1.3 Effective Date September 26, 2018. All employees are responsible for maintaining a safe work environment.

VII. Security Incidents and Investigations

A. Investigations into a security matter may or may not require the involvement of law enforcement. OC San Risk Management in conjunction with Human Resources and applicable OC San Manager(s) or Supervisor(s), and the contracted security service may investigate a security matter when any of the following conditions exists:

1. Administrative inquiries into a matter which violates OC San’s security policies and guidelines or local, state, and federal statutes.

2. Proactive or reactive investigations initiated either primarily for preventive purposes or in response to an act or specific report.

3. Investigations into a procedure or occurrence which require improvements in security protocols and/or standard operating procedures.

4. A security incident report from the current contracted security provider will be completed at the time of incident. When all investigative leads have been followed without success and further investigative action is deemed to be unproductive; or the case may remain open and under investigation by local law enforcement. In some cases, the security incident report may be the final or closing report.

VIII. Communication

A. Communication between Risk Management and employees and our contractors is necessary in maintaining a safe and secure work environment. OC San utilizes various methods of communication strategies to enhance and broaden our approach to and communication network.

B. OC San implements the following strategies to improve and enhance workplace security:

1. OC San utilizes various safety and security committees to discuss security policies and procedures, security related events, and other related issues to improve OC San's security program.

2. New employee orientation(s) on OC San workplace security policies, procedures, and workplace practices.

3. Posted or distributed workplace security bulletins.

4. Utilize various District wide publications such as the SanBox, The Pipeline, and The Digester to inform OC San employees on upcoming security programs and policy initiatives.

5. A mechanism to report security concern or related issue through either SharePoint or another web-based reporting system.

6. Web based and non-web-based training programs.

IX. Access Control

A. OC San utilizes access control technologies to limit and restrict access to OC San wastewater treatment plants, buildings, rooms, and other critical assets which to protect information technology, employee information, and other critical assets that which contribute to the treatment process.

B. All OC San employees and primary contractors will be issued and are required to wear the authorized OC San ID card while on all OC San properties. Employees who work around machinery may place their access card in a secure place on their person during operation to prevent cards from being pulled into machinery which may create risk of injury. ID cards will solely be utilized by individuals who they were issued to.

C. Contractors and/or subcontractors who are not issued identification cards shall be issued temporary identification badges by contracted private security at the designated entry control point at both Plants 1 and 2.

D. No employee or contractor shall allow other individuals to use their issued identification badge to access any OC San facility or structure. The loaning of identification cards could result in disciplinary action in accordance with HR policy(s).

E. No security access control activity log will be released to any employee without the prior approval of the Safety and Health Supervisor or Human Resources and Risk Manager.

F. The ID cards remain property of the Orange County Sanitation District. Persons issued ID cards shall maintain the ID card in good condition, avoid contact with surfaces that can scratch or cause accelerated wear, avoid placing an ID card in the proximity of magnetic sources or fields and ensure that cards are placed in secured location to protect against loss, theft, or unauthorized use.

G. All persons are required to renew their ID card photograph every five (5) years.

H. Employees should ensure that they scan into doors that may already be open prior to entering. This will aid Risk Management, Security, and IT to identify your location in the event of a disaster or other incident.

I. Employees and Contractors shall report the loss or theft of the ID card or the recovery of a lost or stolen ID card to Risk Management. Upon notification, Risk Management will immediately deactivate (block) the lost or stolen ID card from permitting electronic access to all OC San facilities. Risk Management will issue a new card with equivalent credentials.

J. Employees who have been separated from employment or placed on administrative leave or shall return his or her ID card to Risk Management or a Human Resources representative. A Risk Management representative will temporarily suspend electronic access to all OC San facilities.

K. Risk Management is responsible for destroying all returned identification cards.

X. Visitor and Access Control

A. Public Meetings

1. Visitors attending public board meetings which includes the Steering, Administration, Operations Committees, or any other meeting of a legislative body are not required to show identification in accordance with the Brown Act Ch. V § 54953.3. The Brown Act states that visitors attending public meetings “will not be asked to register or identify themselves or pay fees to attend public meetings”.

2. Security will be notified in advanced that a public meeting will be taking place and will prepare generic visitor badges prior to the start of the meeting.

B. Visitors

1. All visitors must show a government issued photo identification and sign-in prior to entering Plants 1 and 2 and other applicable off-site locations. Visitors must obtain a temporary visitor identification badge by providing one of following identifications to verify or establish identity:

   a. Non-Expired U.S. Driver’s License

   b. Identification card issued by federal, state, or local government agencies, provided it contains a photograph and information including the name, date of birth, sex, height, eye color and address including U.S. Citizen ID Card (INS Form I-97), and ID for use of Resident Citizen in the U.S. (INS Form I-179);

   c. U.S. Passport.

   d. Native American Tribal document

2. Visitors who do not have on their person a valid identification will not be permitted to enter.

3. Visitors must complete an authorized COVID-19 screening prior to entry. Security has ability to initiate screening process via the QR code; however, visitors should be provided the approved Visitor COVID-19 Self Screening Questionnaire 24-hours prior to their visit by the requesting OC San employee.

4. Security will issue the visitor a time activated security badge with the visitor's photo which will change color within 24 hours of issue to show authorized visitation has expired. Security will brief the visitor to turn in their temporary badge when leaving the plant.

5. The OC San Visitor Registration System will be the system in which all visitors to include subcontractors will be entered prior to entry into Plants 1 and 2. OC San employees are required to enter visitors into the system when they become aware that they will be visiting either Plants 1 or 2. Security will turn away any persons who are not in the Visitor Registration System and who cannot be verified by an OC San employee.

6. Visitors attending a "tour" will be issued a generic "TOUR" badge with no expiration date and will be granted access to the plant with minimal delay. Tours includes individuals or groups who desire to visit the plant for personal or educational reasons. Such visits may be desired by educational, regulatory, technical, or scientific organizations.

7. Temporary visitor identification badges and parking permits are required for package delivery service drivers which included but is not limited to FedEx, UPS, or the United States Parcel Service.

8. Temporary visitor identification badges are not required for first responders responding to an incident or emergency.

9. OC San employees will work with their assigned contractors to ensure that all sub-contractors are entered into the visitor registration system. Security will be responsible for verifying that the sub-contractor is authorized prior to entering the Plant. Security will verify and process their identification prior to entry. Subcontractors are required to check in with Plant Operations prior to beginning their work assignment.

10. Subcontractors will be issued a temporary visitors' badge with their name, picture, organization or place of business, and the expiration date when their work is expected to be completed. Additionally, the subcontractor will be issued an orange Multi Day Parking Permit which will be set to expire within 30 days of issue or the date their work assignment will be completed; whichever comes first.

C. Facility Protection

1. General

a. OC San takes a strategic approach to physical protection using specifically defined areas with increased levels of security according to the Physical Security Plan. There are two defined security areas: Protected Process Area (PPA) and Vital Operation Area (VOA). Protection of critical facilities involves access control, door alarms, signage, CCTV, or other types of physical and technological barriers which, deter, deny, or restrict access to individuals or groups of individuals who may want to inflict harm to OC San employees, contractors, and visitors. OC San employees and contractors are responsible for maintaining the safety and security of all OC San's facilities throughout the service area.

b. Employees and Contractors shall notify the Plant No. 2 Operations Center at (714) 593-7625 prior to obtaining access to all OC San Pump Stations.

2. After Hour Access and Reporting

a. All visitors scheduled to enter OC San treatment plants after hours shall be entered into the OC San visitor management system located on the SharePoint. Individuals shall notify Risk Management when scheduling after-hour access for all employees, contractors, and other visitors Operations shall also be notified a minimum of 24-hours in advance prior to accessing OC San plant process areas during non-business hours and visitors shall check in with the Control or Operations Center(s) prior to reporting to their job site or office Normal business hours are 6:00am to 5:00pm Monday through Friday (M-F). Contractor Gates are generally open from 5:30am to 3:30pm; however, hours may vary due to the needs of OC San.

b. The Operations Control Center Technician at Plant 1 can be reached at (714) 593- 7025; the Operations Technician at Plant 2 can be reached at (714) 593-7625. The Operations Control Center Technician will enter the information into the operations log and make the appropriate notifications to Operations staff.

c. Contractors and OC San Operations coordinate activities at weekly planning meetings and/or by email exchange to discuss any potential impacts to evening and nighttime plant operations. Names, dates, and contact information should be provided by the contractor to O&M Management when coordinating access during non-business hours. O&M is responsible for the notifying all applicable parties to include Supervisors or Operators who will be affected or involved.

d. If a work activity or site visit must occur outside of the scheduled environment of the weekly planning meetings, the responsible party will contact the Operations or Control Center and/or the Operations supervisor or his designee at the appropriate facility and obtain authorization to proceed prior to the entrance of external staff into the treatment facility process.

3. Vital Operation Areas

a. The following areas have been designated as vital operation areas (VOA), which contain additional security protections as mentioned above:

1) VOA facilities at Plant One:

- Control Center Room
- Central Power Generation Facility
- Power building 2
- Power building 3A
- Power building 4
- Power building 5
- Power building 6
- Power building 7
- Power building 8

- 12Kv Service Center
- Blower Building Turbine Generator Room

2) VOA facilities at Plant Two:

- 12Kv Distribution Center C
- 12Kv Distribution center A
- 12KV Distribution Center B
- 12KV Distribution Center D
- 12Kv Electrical Service Center
- Central Power Generation Building
- Distribution Center H
- Distribution Center J
- Distribution Center K
- EPSA Electrical Building
- EPSA Standby Power Building
- Headwork's Standby Power
- Headworks Power Building A
- headworks power building b
- Operation Center
- PDF Building
- Power Building b
- Power Building C
- Power Building D
- Primary Power Building A
- SBF Electrical Building
- Water In (influent pump station)
- Water Out (OOBS, EPSA)
- Warehouse
- City Water Station
- Gas Compressor Building

b. OC San employees are responsible in the securing of all OC San facility and shall abide by all access control procedures in accordance with this SOP.

XI. Parking Permits, Traffic Control, and Parking

A. Parking Permits

1. OC San employees and contractors shall clearly display issued parking permits on the rearview mirror of their vehicle while operating a motor vehicle or parked on OC San property. Individuals may place permits on the driver's side of the dashboard if vehicle does not have a rearview mirror. The purpose of the parking permit is for the safety and security of all OC San employees, visitors, and contractors. Visible parking permits aid security in authorizing access to designated personnel.

2. The following long-term and temporary parking permits are authorized on OC San property:

a. OC San Employee (Yellow Placard or Sticker)

b. OC San Contractor (Red Placard or Sticker)

c. VIPs (Blue Placard or Sticker)

d. Temporary Long-term (Orange Placard or Sticker)

e. Temporary Single Day Parking Permit (Yellow 24-Hour Card)

f. Temporary 30-Day Parking Permit (Orange 30-day Card)

B. Traffic Control and Parking

1. Unless posted, the speed limit throughout Plants 1 and 2 is 15 miles per hour (mph). Some roadways in the plants are 10 mph. All vehicles will follow all posted traffic control signs. Employees should report traffic control violations if necessary.

2. OC San vehicles shall be operated in compliance with all applicable state and local laws and ordinances. The consequences for failing to comply with any law, regulations, or ordinance, such as speeding citations or toll road fines, will be the responsibility of the driver. Drivers who are found to have violated posted speed limits while driving on OC San property or find any indications of misconduct involving vehicles may be grounds for disciplinary action up to and including termination. It is the intent of this policy that unsafe behavior be identified and corrected. Should discipline become necessary, it will follow the OC San Personnel Policies and Procedures Manual and Memorandum of Understanding (MOU), as applicable.

3. All OC San employees, whether full-time or part-time, including OC San hired contractors must provide OC San with the state issued vehicle license plate number, vehicle year, make, and model of the personal or commercial vehicle(s) they intend to drive and/or park on OC San property. Parking permits will not be issued without first providing OC San with a state issued vehicle license plate number.

4. If Reflective Parking Permits are authorized and are in use, they will be placed inside of the windshield located on the top left driver’s side.

5. Parking permits are not required for non-motorized vehicles, motorcycles, or scooters. All non-motorized vehicles will be required to provide their license plate number to Risk Management and will be logged into the badge control system so that their vehicle can be identified when on site. All motorized vehicles will be required to show security their OC San identification prior to entering Plants 1 and 2.

6. Personal vehicles or OC San Fleet vehicles will not block fire hydrants or park in designated fire lanes. Handicap parking spaces are not to be utilized by a vehicle unless they possess a disabled person placard or license plate.

7. No vehicle will be parked to interfere with or impede the normal flow of traffic or operation of the facilities or otherwise present a traffic hazard.

8. There is no overnight parking of personal vehicles in any OC San parking lot, unless prior clearance has been obtained from Risk Management. Exceptions include those employees who are on OC San work related overnight travel. If on overnight travel, advise security of the location, make, and model of the vehicle.

9. There is no overnight parking of personal vehicles at any pump station.

10. Only contractors, subcontractors and their employees may park within designated construction parking areas.

11. OC San vehicles shall be parked and locked in assigned parking spaces or designated areas.

12. OC San vehicle keys are to remain in a key box located in a secure area.

13. Employees who take OC San Fleet Vehicles home while on call shall park vehicle in covered carports, garages, or driveways is possible. Parking on city or private streets should be avoided.

XII. Civil Demonstrations

A. Civil demonstrations can range from mildly disruptive activities, such as peaceful picketing, to violent and uncontrolled events, including civil unrest and looting.

B. Risk Management will work with the PAO to advertise and distribute current information on civil demonstrations within our area of operations. OC San Risk Management and the Public Affairs Office will monitor civil demonstrations and communicate with the local police agencies as required.

C. OC San employees and contractors should avoid interacting with demonstrators.

XIII. Man-Made Threats

A. OC San employees, contractors, and contracted security will respond to man-made threats utilizing procedures identified in the OC San Integrated Emergency Response Plan (IERP), Annex 5 (Manmade Threats).

B. Manmade Threats include the following:

1. Terrorism

2. Insider Treats

3. Active Shooter

4. Bomb Threats

XIV. Recordkeeping

All records created or generated during this procedure shall be legible and stored in a way that they are readily retrievable in facilities or electronic document/content management systems that provide a suitable environment to prevent damage, deterioration, or loss. Records may be in the form of any type of media, such as hard copy or electronic media. The OC San Records Retention Schedule is the official procedure governing the retention, retirement, and destruction of OC San records. Document owners should use these schedules to determine the item and series that best fit their records. Document owners are responsible for ensuring that documents are properly marked, indexed, and filed for their projects or area of responsibility.

XV. References

Policy F80, Workplace Violence and Weapons

Policy 5.18, Use of District Property

Policy 5.19, Vehicle Usage

Integrated Emergency Response Plan (IERP)

Department of Homeland Security Ensuring Building Security Purpose

XVI. Revision History

Version	Date	By	Reason
1.0	09/14/220	Rivera, George	New
2.0	08/11/2020	Harp, Derek	Periodic Update – Refer to Program Change Log
3.0	12/13/2021	Frattali, John; Harp, Derek	Annual Program Review – No changes with exception to rebrand.