

COMMISSION ON POLICE PRACTICES AGENDA

Saturday, October 14, 2023

10:00am-3pm

REGULAR MEETING (Hybrid)

Mira Mesa Public Library

8405 New Salem Street

San Diego, CA 92126

Commissioners: Octavio Aguilar, Laila Aziz, Bonnie Benitez, Alec Beyer, Dennis W. Brown, Cheryl Canson, Doug Case, Christina Griffin-Jones, Dwayne Harvey, Brandon Hilpert, Darlann Hctor Mulmat, Clovis Honore, James Justus, Dennis Larkin, Lupe Diaz, Mark Maddox, Nicole Murray-Ramirez, Yvania Rubio, Jaylene Sanchez, Gloria Tran, and Dalia Sherlyn Villa De La Cruz

Staff: Interim Executive Director Sharmaine Moseley, Outside Counsel Duane Bennett, Chief Investigator Olga Golub, Community Engagement Coordinator Yasmeen Obeid, Executive Assistant Alina Conde, Administrative Assistant Jon'Nae McFarland

The Commission on Police Practices (Commission) meetings will be conducted pursuant to the provisions of California Government Code Section 54953 (a), as amended by Assembly Bill 2249.

The Commission business meetings will be in person and the meeting will be open for in-person testimony. Additionally, we are continuing to provide alternatives to in-person attendance for participating in our meetings.

In lieu of in-person attendance, members of the public may also participate via telephone/Zoom. Please see instructions below to provide public comment.

The link to join the meeting by computer, tablet, or smartphone at 10am is:

<https://sandiego.zoomgov.com/s/1612777224>

Meeting ID: 161 277 7224

In-Person Public Comment on an Agenda Item: If you wish to address the Commission on an item on today's agenda, please complete and submit a speaker slip before the Commission hears the agenda item. You will be called at the time the item is heard. Each speaker must file a speaker slip with the Executive Director at the meeting at which the speaker wishes to speak indicating which item they wish to speak on. Speaker slips may not be turned in prior to the day of the meeting or after completion of in-person testimony. In-person public comment

will conclude before virtual testimony begins. Each speaker who wishes to address the Commission must state who they are representing if they represent an organization or another person.

For discussion and information items each speaker may speak up to three (3) minutes, subject to the Chair's determination of the time available for meeting management purposes, in addition to any time ceded by other members of the public who are present at the meeting and have submitted a speaker slip ceding their time. These speaker slips should be submitted together at one time to the Executive Director. The Chair may also limit organized group presentations of five or more people to 15 minutes or less.

In-Person Public Comment on Matters Not on the Agenda: You may address the Commission on any matter not listed on today's agenda. Please complete and submit a speaker slip. However, California's open meeting laws do not permit the Commission to discuss or take any action on the matter at today's meeting. At its discretion, the Commission may add the item to a future meeting agenda or refer the matter to staff or committee. Public comments are limited to three minutes per speaker. At the discretion of the Chair, if a large number of people wish to speak on the same item, comments may be limited to a set period of time per item to appropriately manage the meeting and ensure the Commission has time to consider all the agenda items. A member of the public may only provide one comment per agenda item. In-person public comment on items not on the agenda will conclude before virtual testimony begins.

Virtual Platform Public Comment to a Particular Item or Matters Not on the Agenda: When the Chair introduces the item you would like to comment on (or indicates it is time for Non-Agenda Public Comment), raise your hand by either tapping the "Raise Your Hand" button on your computer, tablet, or Smartphone, or by dialing *9 on your phone. You will be taken in the order in which you raised your hand. You may only speak once on a particular item. When the Chair indicates it is your turn to speak, click the unmute prompt that will appear on your computer, tablet or Smartphone, or dial *6 on your phone. The virtual queue will close when the last virtual speaker finishes speaking or 5 minutes after in-person testimony ends, whichever happens first.

Written Comment through Webform: Comment on agenda items and non-agenda public comment may also be submitted using the [webform](#). If using the webform, indicate the agenda item number you wish to submit a comment for. All webform comments are limited to 200 words. On the [webform](#), members of the public should select Commission on Police Practices (even if the public comment is for a Commission on Police Practices Committee meeting).

The public may attend a meeting when scheduled by following the attendee meeting link provided above. To view a meeting archive video, click [here](#). Video footage of each Commission meeting is posted online [here](#) within 24-48 hours of the conclusion of the meeting.

Comments received no later than 11am the day of the meeting will be distributed to the Commission on Police Practices and posted online with the meeting materials. Comments received after the deadlines described above but before the item is called will be submitted into the written record for the relevant item. Please contact the Privacy Advisory Board website for further instructions.

Written Materials: Instead of submitting written materials as an attachment to the webform, you may submit via U.S. Mail to Attn: Office of the Commission on Police Practices, 1200 Third Avenue, San Diego, CA 92101. Materials submitted via U.S. Mail must be received the business day prior to the meeting to be distributed to the Commission on Police Practices.

If you attach any documents to your comment, they will be distributed to the Commission or Committee in accordance with the deadlines described above.

- I. **10:00am** CALL TO ORDER/WELCOME (**5 minutes**)
(Chair Gloria Tran & 1 Vice Chair Dennis Brown)
- II. **10:05am** ROLL CALL (Administrative Assistant Jon’Nae McFarland)
(**5 minutes**)
- III. PURPOSE OF THE COMMISSION ON POLICE PRACTICES
The purpose of the Commission on Police Practices (CPP or Commission) is to provide independent community oversight of SDPD, directed at increasing community trust in SDPD & increasing safety for community and officers. The purpose of the Commission is also to perform independent investigations of officer-involved shootings, in-custody deaths and other significant incidents, and an unbiased evaluation of all complaints against members of SDPD and its personnel in a process that will be transparent and accountable to the community. Lastly, the Commission also evaluates the review of all SDPD policies, practices, trainings, and protocols and represents the community in making recommendations for changes.
- IV. **10:10am** APPROVAL OF MEETING MINUTES (Chair Tran) (**5 minutes**)
 1. CPP Regular Meeting Minutes of October 7, 2023
- V. **10:15am** NON- AGENDA PUBLIC COMMENT (**15 minutes**)
Fill out and submit
comment using speaker form or [webform](#). Please see
instructions at the beginning of this agenda.
(Community Engagement Coordinator Yasmeen Obeid)
- VI. **10:30am** CLOSED SESSION (Lunch provided for Commissioners) (**2 hours**)
(**Not Open to the Public**)
 1. PUBLIC EMPLOYEE DISCIPLINE/DISMISSAL/RELEASE
Discussion & Consideration of Complaints & Reports:
Pursuant to Government Code Section 54957 to discuss
complaints, charges, investigations, and discipline (unless
the employee requests an open public session) involving

San Diego Police Department employees, and information deemed confidential under Penal Code Sections 832.5–832.8 and Evidence Code Section 1040. Reportable actions for the Closed Session items on the agenda will be posted on the Commission’s website at www.sandiego.gov/cpp and when the Commission reconvenes this meeting as listed on this agenda.

- I. San Diego Police Department Feedback on Case Specific Matters
- II. Shooting Review Board Reports (0)
- III. Category II Case Audit Reports (0)
- IV. Discipline Reports (0)
- V. Case Review Team Reports (3)
- VI. Case-Specific Recommendations to the Mayor/Chief (0)
- VII. Referrals to other governmental agencies authorized to investigate activities of a law enforcement agency (0)
- VIII. Legal Opinion(s) Request & Response (0)

- VII. **12:30pm** REPORT FROM CLOSED SESSION (Counsel Bennett) **(5 minutes)**
- VIII. **12:35pm** EDUCATIONAL TOPICS **(30 minutes)**
 - 1. **“Racial Profiling in SDPD”**
Presenter: American Civil Liberties Union (ACLU)
- IX. **1:05pm** AD HOC COMMITTEE REPORTS **(15 minutes)**
 - 1. Bylaws Committee Update
 - 2. Operational Committee Update
 - 3. Training Committee Update
 - 4. Personnel Committee Update
- X. **1:20pm** OFFICE OF THE COMMISSION ON POLICE PRACTICES
 - 1. Introduction/Remarks CPP Chief Investigator **(Olga Golub– 5 minutes)**
 - 2. Community Engagement Coordinator Report **(Yasmeen Obeid - 15 minutes)**
- XI. **1:40pm** NEW BUSINESS (DISCUSSION/ACTION)
 - 1. Plan for Upcoming Case Review Deadlines **(Action Item)**
30 minutes
 - 2 Case Reviews Must be Completed by November 7th Meeting of the Commission **(November)**
 - 5 Case Reviews Must be Completed **(December)**

Motion: Chief Investigator and Commissioners Review Cases According to 1 Year Statutory Limitation Deadlines with the Assistance of Outside Counsel & Experienced Commissioners

2. **2:10pm** Distribution of Laptops to Commissioners
(OCPD Staff)
3. **2:30pm** City of San Diego Administrative Regulations
(Outside Counsel Duane Bennett)
 - a. AR 90.63 City Info Security Policy
 - b. AR 90.62 Information & Communication
 - c. AR 95.60 Conflict of Interest & Employee Conduct
 - d. AR 96.50 EEO Policy & Complaint Resolution
Procedures

XII. ADJOURNMENT

Materials Provided:

- Minutes from Regular Meeting on October 7, 2023 DRAFT
- AR 90.63 City Info Security Policy
- AR 90.62 Information & Communication
- AR 95.60 Conflict of Interest & Employee Conduct
- AR 96.50 EEO Policy & Complaint Resolution Procedures
- Updated Commission Component Training Schedule DRAFT

Access for People with Disabilities: As required by the Americans with Disabilities Act (ADA), requests for agenda information to be made available in alternative formats, and any requests for disability-related modifications or accommodations required to facilitate meeting participation, including requests for alternatives to observing meetings and offering public comment as noted above, may be made by contacting the Commission at (619) 236-6296 or commissionpolicepractices@saniego.gov.

Requests for disability-related modifications or accommodations required to facilitate meeting participation, including requests for auxiliary aids, services, or interpreters, require different lead times, ranging from five business days to two weeks. Please keep this in mind and provide as much advance notice as possible in order to ensure availability. The city is committed to resolving accessibility requests swiftly in order to maximize accessibility.

Office of the Commission on Police Practices

**COMMISSION ON POLICE PRACTICES
REGULAR MEETING MINUTES**

Tuesday, October 7, 2023

10:00am

Logan Heights Branch Library

567 S 28th Street

San Diego, CA 92113

Click <https://youtu.be/tsJqiqh9ENC> to view this meeting on YouTube.

Commissioners Present:

Chair Gloria Tran

1st Vice Chair, Dennis W. Brown

2nd Vice Chair, Doug Case

Octavio Aguilar

Laila Aziz

Bonnie Benitez

Alec Beyer

Cheryl Canson

Dwayne Harvey

Brandon Hilpert

Darlanne Hocter-Mulmat

Clovis Honore

James Justus

Dennis Larkin

Lupe Lozano-Diaz

Mark Maddox

Yvania Rubio

Absent/Excused:

Nicole Murray-Ramirez

Jaylene Sanchez

Christina Griffin-Jones

Dalia Sherlyn Villa De La Cruz

Staff Present:

Sharmaine Moseley, Interim Executive Director

Duane Bennett, CPP Outside Counsel

Olga Golub, Chief Investigator

Yasmeen Obeid, Community Engagement Coordinator

Alina Conde, Executive Assistant

Jon'Nae McFarland, Administrative Assistant

-
- I. CALL TO ORDER/WELCOME: Chair Gloria Tran called the meeting to order at 10:05am.
 - A. Chair Tran shared highlights from the Chair Report (attached to the minutes).

- II. ROLL CALL: Interim Executive Director Sharmaine Moseley conducted the roll call.
- III. PURPOSE OF THE COMMISSION ON POLICE PRACTICES: The purpose of the Commission on Police Practices (CPP or Commission) is to provide independent community oversight of SDPD, directed at increasing community trust in SDPD & increasing safety for community and officers. The purpose of the Commission is also to perform independent investigations of officer-involved shootings, in-custody deaths and other significant incidents, and an unbiased evaluation of all complaints against members of SDPD and its personnel in a process that will be transparent and accountable to the community. Lastly, the Commission also evaluates the review of all SDPD policies, practices, trainings, and protocols and represents the community in making recommendations for changes.
- IV. APPROVAL OF MEETING MINUTES
- A. CPP Regular Meeting Minutes of September 12, 2023
Motion: Commissioner James Justus moved for the Commission to approve the amended CPP Regular Meeting Minutes of September 12, 2023. Commissioner Alec Beyer seconded the motion. The motion passed with a vote of 17-0-0.
Yays: Chair Tran, 1st Vice Chair Brown, 2nd Vice Chair Case, Aziz, Aguilar, Benitez, Beyer, Canson, Harvey, Hilpert, Hocter-Mulmat, Honore, Justus, Larkin, Lozano-Diaz, Maddox, and Rubio
Nays: None
Abstained: None
Absent/Excused: Griffin-Jones, Murray-Ramirez, Sanchez, and Villa De La Cruz
- B. CPP Regular Meeting Minutes of September 19, 2023
Motion: Commissioner Bonnie Benitez moved for the Commission to approve the amended CPP Regular Meeting Minutes of September 19, 2023. Commissioner Alec Beyer seconded the motion. The motion passed with a vote of 17-0-0.
Yays: Chair Tran, 1st Vice Chair Brown, 2nd Vice Chair Case, Aziz, Aguilar, Benitez, Beyer, Canson, Harvey, Hilpert, Hocter-Mulmat, Honore, Justus, Larkin, Lozano-Diaz, Maddox, and Rubio
Nays: None
Abstained: None
Absent/Excused: Griffin-Jones, Murray-Ramirez, Sanchez, and Villa De La Cruz
- V. NON-AGENDA PUBLIC COMMENT: No public comment received.
- VI. NEW BUSINESS (DISCUSSION/ACTION) – None
- VII. EDUCATIONAL TOPICS
- A. Outside Counsel Duane Bennet presented an overview of the Ralph M. Brown act. **Audio was cut off due to technical issues from (Timestamp 14:37-27:30). Please see the attached PowerPoints for the presentations.* Outside Counsel Duane Bennett presented on closed sessions and the duty/requirement of confidentiality and impartiality.
In-person Public Comment: None

Virtual Public Comment:

Brandie James (Timestamp 37:11) references San Diego Police Department's policies and procedures 1.10. Requesting confirmation of CPP review of investigations.

Darwin Fishman (Timestamp 39:52) comments the history of the CRB voting in favor of IA Findings. Encourages CPP to be independent and to use the tools that are available.

- B. 2nd Vice Chair Case and Outside Counsel Duane Bennet presented on "How to Review a Case." (Timestamp 44:30) 2nd Vice Chair Doug Case presented on complaints and internal affairs process. Outside Counsel Duane Bennett presented on CPP Review of cases.

In-person Public Comment: None

Virtual Public Comment:

Francine Maxwell (Timestamp 1:06:22) would like clarification on whether the CPP will still conduct an internal investigation even if the subject officer has resigned.

Brandie James (Timestamp 1:08:02) requests clarification on whether the CPP investigates all IA complaints or only IA complaints that could lead to an appeal.

- C. Outside Counsel Duane Bennett presented on the topic of Fourth Amendment: Searches, Arrests, and Use of Force. (Timestamp 1:16:30)

In-person Public Comment: None

Virtual Public Comment:

Darwin Fishman (Timestamp 1:49:40) spoke about the CPP not taking action regarding the banning of the Carotid Restraint.

**In the Citizens' Review Board (CRB) meeting of October 30, 2018, the board made a recommendation to remove the Carotid Restraint from SDPD's Use of Force Department Procedure 1.04.*

Recommendation that SDPD remove the Carotid Restraint from SDPD's Use of Force Department Procedure 1.04 for Active Resistance Behavior and retain for Assaultive or Life-Threatening Behavior. If SDPD uses the Carotid Restraint on a person, the person must be transferred immediately to a medical facility - Chief Nisleit explained why he will not remove the carotid restraint as a tool for officers to use when someone engages in Active Resistance. He explained that when you remove a lower-level force option, the officers would have to take it up a notch using a higher-level force option. Chief Nisleit explained the difference between the chokehold and carotid restraint. The chokehold uses front neck pressure that cuts off the air supply and the carotid restraint restricts the vascular veins of the neck cutting off blood flow which renders the person unconscious fast. The City of San Diego has not had any deaths from the carotid restraint being applied since 1992. It is a two-officer technique.

<https://www.sandiego.gov/sites/default/files/crbminutes181030.pdf>

VIII. Break/Lunch

IX. CLOSED SESSION (NOT OPEN TO THE PUBLIC)

A. PUBLIC EMPLOYEE DISCIPLINE/DISMISSAL/RELEASE

Discussion & Consideration of Complaints & Reports: Pursuant to Government Code Section 54957 to discuss complaints, charges, investigations, and discipline (unless the employee requests an open public session) involving San Diego Police Department employees, and information deemed confidential under Penal Code Sections 832.5-832.8 and Evidence Code Section 1040. Reportable

actions for the Closed Session items on the agenda will be posted on the Commission's website at www.sandiego.gov/cpp or stated at the beginning of the Open Session meeting if the meeting is held on the same day.

- I. San Diego Police Department Feedback on Case Specific Matters
- II. Shooting Review Board Reports (0)
- III. Category II Case Audit Reports (0)
- IV. Discipline Reports (0)
- V. Case Review Team Reports (3)
- VI. Case-Specific Recommendations to the Mayor/Chief (0)
- VII. Referrals to other governmental agencies authorized to investigate activities of a law enforcement agency (0)
- VIII. Legal Opinion(s) Request & Response (0)

- X. REPORT OUT FROM CLOSED SESSION: (3:27pm): Outside Counsel Duane Bennett reported that the Commission voted unanimously to add open agenda items for discussion. 2nd Vice Chair Doug Case explained that the agreement was to add trainings to future meetings. Additionally, to add one or more community forum(s) by June 30th, 2024, regarding SDPD's policies and practices on pretextual stops, 4th amendment waiver searches, the Special Operations Unit methodologies, and de-escalation policies and trainings. SDPD Leadership should be invited to participate. The purpose of the forums is to inform the Commission on developing recommendations for these issues.
- XI. ADJOURNMENT: The meeting was adjourned at 3:29pm.



Commission on Police Practices

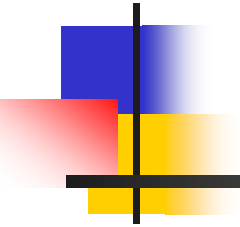
Chair Report
October 7, 2023

Here is a brief summary of what the CPP and its Cabinet have accomplished since being sworn in on August 29, 2023.

- The 4 Ad Hoc Committees have met and elected chairs. Thank you to those who have taken on leadership roles:
 - Bylaws Ad Hoc Committee, chaired by Commissioner Mark Maddox
 - Operating Procedures Ad Hoc Committee, co-chaired by Commissioner Yvania Rubio and Second Vice Chair Doug Case
 - Ad Hoc Personnel Committee, chaired by First Vice Chair Dennis Brown
 - Ad Hoc Training Committee, chaired by Commissioner Brandon Hilpert
- The Cabinet and Interim Executive Director communicate every day to follow through on motions passed by Commissioners and get the new CPP organized.
- We are working on making the CPP more efficient by putting time limits on comments in order to complete Commission business.
- The Cabinet, Ms. Moseley, and Mr. Bennett reported to the Public Safety Committee on September 20.
 - We were reported that we held 3 meetings since taking the oath of Commissioner.
 - The CPP voted to retain a Contract Investigator to audit cases over one year to look for trends or patterns that may be addressed.
- The Cabinet has meetings scheduled with Police Chief David Nisleit on October 25th, and Public Safety Committee chair Marni Von Wilpert on November 1st, and we are in the process of scheduling a meeting with the City Council president, Sean Elo-Rivera.
- The Cabinet and Interim Executive Director will attend the National Association for Civilian Oversight of Law Enforcement or NACOLE annual conference in mid-November in Chicago.
- The CPP Leadership Team is planning future meetings and trainings, as well as working to ensure no more cases expire.
- Commissioners who signed the Confidentiality Agreement were given access to view the Internal Affairs Google Drive in preparation for today's case review.
- Commissioners will get city laptops at our meeting on Oct. 14, and training on how to use them.
- We are working to set a permanent meeting location and dates.

Gloria Tran, Chair
Commission on Police Practices

Closed Sessions and the Duty/Requirement of Confidentiality and Impartiality





Closed Sessions are Exceptions to Open Meeting Requirements

- Personnel Matters: appointment, evaluation, discipline, dismissal (unless requested by employee to be done in public)
- Existing Litigation, threatened litigation or anticipated litigation
- Labor Negotiations: salaries, benefits...
- Public Security: imminent threats to public safety



Police Officer Personnel Files Are Confidential

Penal Code sections 832.5 and 832.8: Complaints against officers and personal information

Penal Code sec. 835.7:

(a) Except as provided in subdivision (b), the personnel records of peace officers and custodial officers and records maintained by a state or local agency pursuant to Section 832.5, or information obtained from these records, are confidential and shall not be disclosed in any criminal or civil proceeding except by discovery pursuant to Sections 1043 and 1046 of the Evidence Code. This section does not apply to investigations or proceedings concerning the conduct of peace officers or custodial officers, or an agency or department that employs those officers...



Penal Code section 832.7

... the following peace officer or custodial officer personnel records and records maintained by a state or local agency shall not be confidential and shall be made available for public inspection...

(A) A record relating to the report, investigation, or findings of any of the following:

(i) An incident involving the discharge of a firearm at a person by a peace officer or custodial officer.

(ii) An incident involving the use of force against a person by a peace officer or custodial officer that resulted in death or in great bodily injury.

(iii) A sustained finding involving a complaint that alleges unreasonable or excessive force.

(iv) A sustained finding that an officer failed to intervene against another officer using force that is clearly unreasonable or excessive.

(B) (i) Any record relating to an incident in which a sustained finding was made by any law enforcement agency or oversight agency that a peace officer or custodial officer engaged in sexual assault involving a member of the public.



Penal Code section 832.7 (Cont.)

(C) Any record relating to an incident in which a sustained finding was made by any law enforcement agency or oversight agency involving dishonesty by a peace officer or custodial officer directly relating to the reporting, investigation, or prosecution of a crime, or directly relating to the reporting of, or investigation of misconduct by, another peace officer or custodial officer, including, but not limited to, false statements, filing false reports, destruction, falsifying, or concealing of evidence, or perjury.

(D) Any record relating to an incident in which a sustained finding was made by any law enforcement agency or oversight agency that a peace officer or custodial officer engaged in conduct including, but not limited to, verbal statements, writings, online posts, recordings, and gestures, involving prejudice or discrimination against a person on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status.

(E) Any record relating to an incident in which a sustained finding was made by any law enforcement agency or oversight agency that the peace officer made an unlawful arrest or conducted an unlawful search.



Police Officer Confidentiality (Penal Code 832.7)

6) An agency shall redact a record disclosed pursuant to this section only for any of the following purposes:

(A) To remove personal data or information, such as a home address, telephone number, or identities of family members, other than the names and work-related information of peace and custodial officers.

(B) To preserve the anonymity of whistleblowers, complainants, victims, and witnesses.

(C) To protect confidential medical, financial, or other information of which disclosure is specifically prohibited by federal law or would cause an unwarranted invasion of personal privacy that clearly outweighs the strong public interest in records about possible misconduct and use of force by peace officers and custodial officers.

(D) Where there is a specific, articulable, and particularized reason to believe that disclosure of the record would pose a significant danger to the physical safety of the peace officer, custodial officer, or another person.

(7) Notwithstanding paragraph (6), an agency may redact a record disclosed pursuant to this section, including personal identifying information, where, on the facts of the particular case, the public interest served by not disclosing the information clearly outweighs the public interest served by disclosure of the information.



Government Code Section 54957(b)(2)

“As a condition to holding a closed session on specific complaints or charges brought against an employee by another person or employee, the employee shall be given written notice of his or her right to have the complaints or charges heard in an open session rather than a closed session, which notice shall be delivered to the employee personally or by mail at least 24 hours before the time for holding the session. If notice is not given, any disciplinary or other action taken by the legislative body against the employee based on the specific complaints or charges in the closed session shall be null and void.”



Confidentiality Under the Brown Act

- Government Code section 54963 was enacted to penalize “leaks” of confidential information from closed sessions
- Unauthorized communications may constitute misdemeanor violations as determined by the grand jury



Government Code Section 54963

“(a) A person may not disclose confidential information that has been acquired by being present in a closed session authorized...to a person not entitled to receive it, unless the legislative body authorizes disclosure of that confidential information.”



ILLEGAL PUBLIC DISCLOSURE

- Since the legislative body holds a privilege of non-disclosure, only the body (Board) may authorize public disclosure of closed session discussions where “reportable action ” has not occurred



Brown Act Sanctions

- Misdemeanor against each member of a legislative body who:
 1. Attends a meeting of that body
 2. Where action is taken in violation
 3. Where the member intended to deprive the public of information which the member knew the public had a right to receive



Misdemeanor Penalty

1. Confined to meetings where “actions” are taken in violation of the Act, as opposed to where only “deliberation” occurs.
2. Violations may invalidate actions of the commission, investigative findings, disciplinary recommendations, etc.
3. The District Attorney or public may also file a civil action to enjoin violations.



DUTY OF IMPARTIALITY

In holding the SDPD accountable to the public, evaluation and review must be commensurate with:

- Impartiality
- Due Process
- Fairness
- Equal treatment to the Public, Complainants, Officers and Department



Commission Review and Evaluation and Investigative Findings and Discipline

- The CPP makes reviews and makes investigatory and disciplinary findings that could be the subject of appeals
- These functions require objectivity, impartiality, due process, fairness and avoidance of conflicts of interest
- A conflict of interest will exist if extraneous factors influence or dictate a commissioner's actions resulting in a biased decision



Conflicts of Interest

A conflict of interest occurs when personal interests , family, friendships, associations, financial or social factors could influence or compromised judgment, decisions or actions



NACOLE Code of Ethics

(Incorporated by San Diego Municipal Code Section 261106 (c)(7))

1. Personal Integrity;
2. Independent Oversight;
 - Integrity
 - Objective Fairness
 - Impartiality
3. Transparency;
4. Confidentiality;
5. Respectful and Unbiased Treatment;
6. Professional Excellence;
7. Primary Commitment to Community over Personal Interests.



FOURTH AMENDMENT: SEARCHES, ARRESTS AND USE OF FORCE

Fourteenth Amendment, equal protection, liberty, privacy

Section 1

All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of *life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.*

42 U.S.C. SECTION 1983 TEXT AND JURISDICTION

42 U.S.C. §1983 reads as follows:

Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or *the District of Columbia*, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress. For the purposes of this section, any Act of Congress applicable exclusively to the District of Columbia shall be considered to be a statute of the District of Columbia.

THE FOURTH AMENDMENT AS A BASIS OF CIVIL RIGHTS

- The Fourth Amendment prohibits illegal arrests, searches of persons, residences and buildings, as well as uses of unreasonable or excessive force.

Probable Cause is Required for Arrests

- A warrantless arrests requires probable cause
1. **PROBABLE CAUSE**: A reasonable ground for belief in the existence of facts warranting an arrest or search.
 2. **PROBABLE CAUSE** exists where the facts and circumstances would warrant a person of reasonable caution to believe that an offense was or is being committed.
 3. **PROBABLE CAUSE** is the existence of circumstances which would lead a reasonably prudent person to believe in the guilt of the arrested party.

SEARCHES UNDER THE FOURTH AMENDMENT

1. Searches of Persons
2. Searches of vehicles
3. Entries/searches of residences
4. Fourth Waivers

GENERAL RULE REGARDING SEARCHES

- ▶ Pursuant to a warrant
- ▶ Imminent threat
- ▶ Incident to arrest
- ▶ Consent
- ▶ Exigency/Hot pursuit
- ▶ Fourth Waiver

ENTRY INTO RESIDENCES OR BUILDINGS

- In general, law enforcement entries into buildings or residences require a warrant pursuant to the Fourth Amendment.
- Absent a warrant, an exception must exist to justify a warrantless entry.

EXCEPTIONS TO THE WARRANT REQUIREMENT

- ▶ Under the Fourth Amendment, it is necessary that officers enter a residence only upon the existence of a valid search warrant. In the absence of a warrant entries should only be made where:
 - There is express and unequivocal consent (*scope of search is limited by the consent given);
 - Exigent or emergency circumstances exist justifying an immediate entry [even then the exigency should clearly exist and be articulated prior to the entry];
 - Criminal conduct or evidence is in plain view and witnessed by an officer from a location where the officer has authority to be.
 - Fourth Waiver as an exception?

FOURTH WAIVERS

- As a term of probation, a subject may give up a right to privacy by agreeing to be searched without reasonable suspicion – *Fourth Waiver*

The Supreme Court held that when an involuntary search condition is properly imposed, the searching officers are not required to have a reasonable suspicion of criminal activity before conducting the search. "Such a search is reasonable within the meaning of the Fourth Amendment as long as it is not arbitrary, capricious or harassing." (*People v. Reyes, supra*, [19 Cal.4th at p. 752](#).) The Supreme Court held that when an involuntary search condition is properly imposed, the searching officers are not required to have a reasonable suspicion of criminal activity before conducting the search. "Such a search is reasonable within the meaning of the Fourth Amendment as long as it is not arbitrary, capricious or harassing."

SCOPE OF FOURTH WAIVER SEARCHES

- ▶ "It is true that if persons live with a probationer, common or shared areas of their residence may be searched by officers aware of an applicable search condition. [Citations.] Critically, however, cohabitants need not anticipate that officers with no knowledge of the probationer's existence or search condition may freely invade their residence in the absence of a warrant or exigent circumstances. Thus, while cohabitants have no cause to complain of searches that are reasonably and objectively related to the purposes of probation — for example, when routine monitoring occurs [citation] or when facts known to the police indicate a possible probation violation that would justify action pursuant to a known search clause [citation] — they may legitimately challenge those searches that are not." (*People v. Robles*, *supra*, [23 Cal.4th at pp. 798-799.](#))

FOURTH WAIVER RESIDENTIAL SEARCHES

- ▶ The law does not support the proposition that police officers may enter a residential premises, without a warrant and without any awareness of a resident's probation search condition, to indiscriminately search for and seize evidence of suspected criminal wrongdoing.
- ▶ Searches that are undertaken pursuant to a probationer's advance consent must be reasonably related to the purposes of probation.
- ▶ “Significantly, a search of a particular residence cannot be ‘reasonably related’ to a probationary purpose when the officers involved do not even know of a probationer who is sufficiently connected to the residence. Moreover, if officers lack knowledge of a probationer's advance consent when they search the residence, their actions are wholly arbitrary in the sense that they search without legal justification and without any perceived limits to their authority.” (*People v. Robles*, *supra*, [23 Cal.4th at p. 797.](#))

USE OF FORCE

The Fourth Amendment prohibits illegal searches, as well as illegal arrests or “unreasonable seizures.”

By law, excessive force constitutes an “unreasonable seizure” under the Fourth Amendment.

USE OF FORCE AND LAW ENFORCEMENT

Courts continue to define use of force liability in the context of *Graham v. Connor*, 490 U.S. 386 (1989)

- According to *Graham*, “determining whether the force used to effect a particular seizure is ‘reasonable under the Fourth Amendment requires a careful balancing of the nature and quality of the intrusion on the individuals Fourth Amendment interests’ against the countervailing governmental interests at stake.”

Nehad v. Browder, City of San Diego, Zimmerman
929 F.3d 1125 (9th Cir. 2019)

- ▶ “In Fourth Amendment excessive force cases, we examine whether police officers’ actions are objectively reasonable given the totality of the circumstances... Whether a use of force was reasonable will depend on the facts of the particular case, including, but not limited to, whether the suspect posed an immediate threat to anyone, whether the suspect resisted or attempted to evade arrest, and the severity of the crime at issue.”

Graham v. Connor and “Objective Reasonableness”

- ▶ Reasonableness must be judged from the perspective of a reasonable police officer **on the scene, not based on hindsight**, and should take into account the fact that police officers are often forced to make split-second judgments about the amount of force that is necessary in a particular situation.
- ▶ The test for reasonableness is an “**objective**” one that does not depend upon and cannot be influenced by the officer’s underlying intent or motivation for employing force.
- ▶ “An officer’s evil intentions will not make a Fourth Amendment violation out of an objectively reasonable use of force; nor will an officer’s good intentions make an objectively unreasonable use of force constitutional.” **Whether force is used in “good faith” or “maliciously and sadistically for the very purpose of causing harm” was deemed to be irrelevant**, according to the Supreme Court in *Graham v. Connor*.

Force to be Constitutional Must be Reasonable in Light of the Fourth Amendment

Courts analyze several factors in analyzing use of force cases in general:

- ▶ Degree of threat or harm to officers
- ▶ Resistance by the suspect
- ▶ Flight of the suspect
- ▶ Necessity of officers to make split second decisions
- ▶ Threat of harm to the public or others



SDPD USE OF FORCE FACTORS

An officer's decision to use force is based upon the totality of the circumstances and various factors that pertain to officers and/or subjects. These factors include, but are not limited to, the following:

- Age;
- Availability of other options;
- Confined spaces;
- Ground fighting;
- Distance between subject(s) and officer(s);
- Influence of alcohol or drugs;
- Injury/disability;
- Location/terrain/lighting conditions;
- Multiple subjects/officers;
- Nature of offense;
- Opportunity/time for de-escalation;
- Proximity to weapons;
- Size;
- Special knowledge/imminent danger;
- Strength/endurance;
- Type of weapon involved/perceived;
- Crowd control situations.

PENAL CODE SECTION 835

OBJECTIVELY REASONABLE AND NECESSARY FORCE MAY BE USED:

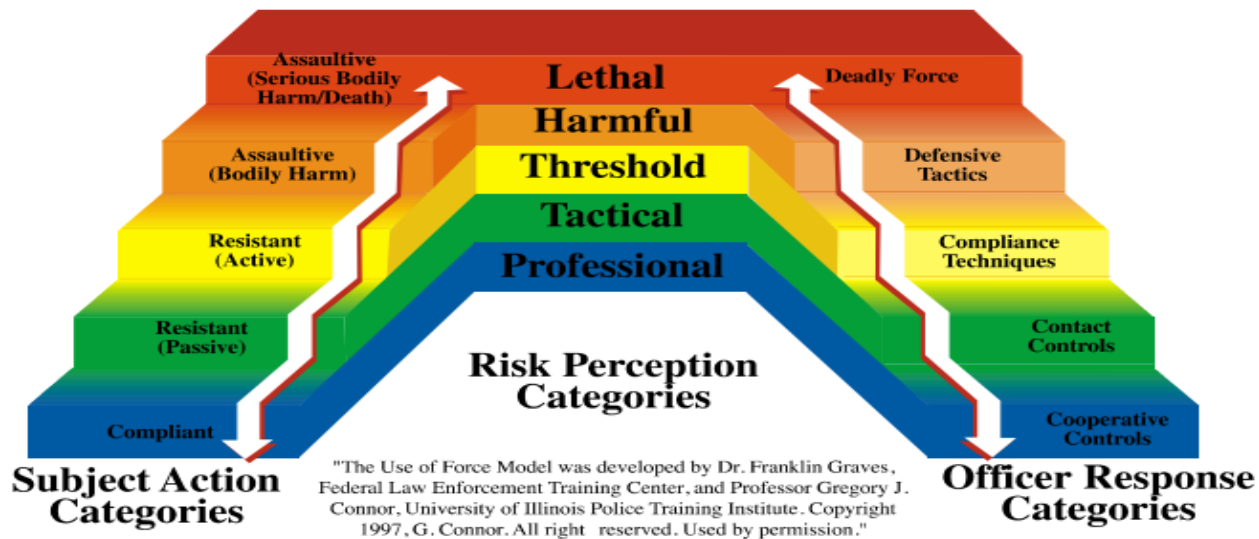
1. To effectuate any arrest;
2. Prevent escape;
3. Overcome resistance.

- A peace officer is justified in using deadly force upon another person only when the officer reasonably believes, based on the totality of the circumstances, that such force is necessary for either of the following reasons:

- ▶ (A) To defend against an imminent threat of death or serious bodily injury to the officer or to another person.
- ▶ (B) To apprehend a fleeing person for any felony that threatened or resulted in death or serious bodily injury, if the officer reasonably believes that the person will cause death or serious bodily injury to another unless immediately apprehended. Where feasible, a peace officer shall, prior to the use of force, make reasonable efforts to identify themselves as a peace officer and to warn that deadly force may be used, unless the officer has objectively reasonable grounds to believe the person is aware of those facts...

Example of Use of Force Continuum

USE OF FORCE MODEL



Eric Garner - "I Can't Breathe" Carotid Restraints



GEORGE FLOYD, EXCESSIVE FORCE AND MURDER

Again, the phrase, "I can't breathe"



EXCESSIVE FORCE IS NOT NECESSARILY ABOUT DISCRIMINATION –TYRE NICHOLS



CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 1 of 12 |
| | Effective Date May 5, 2017 | | |

1. PURPOSE

- 1.1. To ensure *City Information* is accurate, relevant, properly protected, and handled consistent with City policies and *Standards*.
- 1.2. To establish *Information Security Policies* and procedures for protection of *City Information* and the use of *City Computer Equipment*, Network Services, and *Electronic Mail (Email)* and non-City or personal *Computer Equipment* that may be used to access *City Computer Equipment*, *Computer Systems* or *Network Services* by any person or affiliate that is subject to this Administrative Regulation.
- 1.3. To establish a procedure for approving and notifying employees, and other individuals and entities subject to this Administrative Regulation, about *Information Security Standards and Guidelines* that will provide specific guidance and criteria in securing and using *City Computer Equipment*, *Network Services*, and *Email*.
- 1.4. To establish the basis for an Identity Theft Prevention Program, to ensure the security and safety of both employee and citizen/customer personal information.

2. SCOPE

- 2.1. This regulation applies to all City employees, contractors, volunteers, and other affiliates, sometimes collectively referred to as "Individuals," using some or all of the City of San Diego's *Computer Systems*, *Computer Equipment*, *Network Services* or *Email* system.
- 2.2. This regulation applies to the use of *City Computer Equipment* or *Network Services* and to non-City or personal computer equipment that may be used to access *City Computer Systems* or *Network Services* by any Individual subject to this Administrative Regulation.

3. DEFINITIONS

- 3.1. Breach - Means unauthorized access to the City's Computer Equipment, *Computer Systems*, *Email*, or *Network Services* was, or is reasonably believed to have been, acquired by an unauthorized person.

(Supersedes Administrative Regulation 90.63, Issue 1, effective June 30, 2011)

Authorized

(Signature on File)

CHIEF OPERATING OFFICER

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 2 of 12 |
| | Effective Date May 5, 2017 | | |

- 3.2. City Information - Includes information relating to the conduct of the public's business which is prepared, owned, used or retained by any City department or Individual regardless of physical form or characteristics.
- 3.3. Computer Equipment - Includes computer hardware and peripherals, including monitor, mouse, keyboard, and printers, tablets, portable or laptop computers, smart phones and similar communication equipment owned, operated or maintained by the City or an information technology (IT) service provider under contract with the City.
- 3.4. Computer Systems - Includes a network system, interconnected *computer equipment* (e.g., servers and storage devices), software package, or other IT resources.
- 3.5. Email (Electronic Mail) - A method of composing, storing, sending, and receiving (electronic transfer of information) electronic messages, memoranda, and attached documents from a sender to one or more recipients via a telecommunications network.
- 3.6. Guidelines - Recommended actions and/or industry best practices that should be used regarding security practices for ensuring compliance with policies and *standards*.
- 3.7. Information Security - An attribute of information systems which includes specific policy-based mechanisms, practices, procedures, and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services, and the privacy of individuals.
- 3.8. Information Security Standards and Guidelines - Means the *standards* and *guidelines* developed by the Department of IT and approved by the appropriate IT governance body which govern operation of City *Computer Systems*, *Computer Equipment*, *Email*, and *Network Services*.
- 3.9. Information Security Policies - Organizational rules and practices that regulate how an organization manages, protects, and uses its information system assets and data.
- 3.10. Internet - A publicly accessible network connecting *Computer Systems* throughout the world using the standard *Internet* Protocol (IP). In addition to providing capability for *Email*, other *Internet* applications include, but are not limited to, news groups, data processing & storage services, data transfer services, *Email*, cloud services, and the world-wide web ("WWW" or "Web").
- 3.11. Network Services - Communication networks, including the underlying infrastructure of routers, switches, wireless access points, and communications media for hard-wired or wireless transmission of data across the network. Local Area Networks (LANs), Wide Area Networks (WANs), the *Internet*, and wireless networks are examples of *Network Services*.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 3 of 12 |
| | Effective Date May 5, 2017 | | |

- 3.12. Standards - Indicates how and what kind of software, hardware, databases, and business practices should be implemented, used, and maintained to meet security and operational objectives.
- 3.13. System Managers or System Administrators - Individuals who support the operations and integrity of City *Computer Systems* and their use. Their activities might include system installation, configuration, integration, maintenance, security management, and problem analysis and recovery. By the nature of their duties, they have administrative-level access to *Computer Systems*, including operating systems, applications, databases, software utilities, and computer hardware, not accessible by standard *Users*.
- 3.14. User - Any individual who has been granted privileges and access to City *Computer Equipment, Network Services*, applications, resources, or information. *User* is also any person who is identified in Sections 2.1. and 2.2. above.
- 3.15. User ID or User Account - The unique account identifier that is assigned to a *User* of the City's *Computer Equipment, Computer Systems*, and *Network Services*.

4. POLICY

4.1. General

- 4.1.1. Guidance, direction, and authority for *Information Security* activities are centralized for the City under the Department of Information Technology ("Dept. of IT"), Chief *Information Security Officer* (CISO).
- a. The Dept. of IT will provide direction and expertise to ensure the City's information is protected. This responsibility includes consideration of the confidentiality, integrity and availability of both information and *Computer Systems* that manage information. The Dept. of IT will act as a liaison for all *Information Security* matters with all City departments and IT service providers, and must be the focal point for all *Information Security* activities throughout the City. The Dept. of IT will participate in vendor product evaluations and in-house system development projects, assist with implementing security controls, investigate *Information Security Breaches* and perform other activities which are necessary to assure a secure information handling environment.
- b. The Dept. of IT has the authority to provide exceptions to specific provisions of this policy based upon unique business requirements and other considerations. Departments will promptly notify the Dept. of IT in the event an exception is being requested for the security requirements of their respective *Computer Systems*. All exception requests and resulting actions must be fully documented and will be retained by the Dept. of IT.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 4 of 12 |
| | Effective Date May 5, 2017 | | |

- 4.1.2. All computer files developed, created or enhanced within the scope and course of City employment, or a City third-party contractual relationship, are the property of the City of San Diego, regardless of their physical location or the form in which they are maintained. These include, but are not limited to, computer data files, documents, databases, spreadsheets, calendar entries, appointments, tasks, and notes which reside on any City *Computer Systems* or *Computer Equipment*, or the *computer equipment* of a contractor performing work for or on behalf of the City.
- a. The City reserves the right to access and disclose as required or permitted by law, and as defined in the approved *Information Security Standards and Guidelines*, all messages and other electronic data sent over its *Email* systems or stored in computer files on City *Computer Equipment*. City-related computer files stored on non-City or personal computers must be provided upon the City's request in City standard formats.
 - b. It is the responsibility of the Department Head or designee to ensure access to City *Computer Systems* is terminated and all computer files are properly handled by the City when an employee leaves City employment, pursuant to applicable City regulations, policies, and procedures.
 - c. All inventions, improvements, developments, or other works and any related copyrights, trademarks, patents or other intellectual property rights which are in any way related to City business or activities and which are created, developed, enhanced, or are derived, by one or more City employees during the employee's employment and compensated working hours, or using City *Computer Equipment*, or otherwise developed within the scope of an employee's employment, are the exclusive intellectual property rights of the City of San Diego and the City shall own all rights in such intellectual property, including any applicable copyright, patent, trademark, or other intellectual property rights.
- 4.1.3. Access to information available through the City's *Network Services* or from the City's *Computer Systems* is controlled by Dept. of IT approved access control criteria and *Information Security Standards and Guidelines*, which are to be maintained and reviewed at least annually, including updates, as necessary.
- 4.1.4. Authorized access to City *Computer Systems* and *Network Services* shall be at the minimum level required for the Individual to perform and complete their assigned duties, and not at a level that allows access to information beyond the scope of that Individual's assigned duties.
- 4.1.5. Each *Computer System* or *Network Services User ID* must uniquely identify only one *User*. Generic, shared, or group *User IDs* are not permitted. Any unique *User ID* shall not be duplicated across multiple *user* authentication directories,

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 5 of 12 |
| | Effective Date May 5, 2017 | | |

so that there is always only one source *User* directory for authenticating any *User ID* for access to City *Computer Systems* or *Network Services*. Network security groups may be used to combine *Users* access rights. Approved group *Email* accounts may be shared by multiple *Users* who each have unique *User IDs*.

- a. Any Department that requires Individuals to share a single *Computer System*, such as a desktop PC used for customer service, must ensure compliance with the shared-use workstation requirements of the *Information Security Standards and Guidelines*.
- 4.1.6. The initial login password issued to a *User* must be valid only for that *User's* first online session. At the time of initial login, the system must force the *User* to create another password before any other work can be done on the system. Passwords must meet the current criteria set in the *Information Security Standards and Guidelines*.
- 4.1.7. *Network Services* are an essential component of the City's information resources. No device may be connected to the City's *Computer Systems*, data network or voice network unless it has been specifically approved by the Department of Information Technology (IT) pursuant to *Information Security Standards and Guidelines* adopted in accordance with this policy. This section excludes portable data storage devices/media, such as USB drives, being connected to an existing City computer, as long as proper security measures are taken with those devices to prevent and avoid infection by malicious software (i.e., virus or Trojan).
- 4.1.8. All servers, network equipment or telecommunications equipment used for the production support of City business operations must utilize uninterruptible power supply (UPS) and surge protection. Devices deemed critical to City business operations should be on dual power grids or on emergency power generators to protect against power outages.
- 4.1.9. Portable storage devices should only be used for temporary storage of data. Any City data or records created on portable storage devices, such as CDs or USB drives, are to be treated according to Section 4.1.2. above. The content should be made accessible in a standard format and should comply with the *Information Security Standards and Guidelines*. City records stored on portable storage devices must be retained in accordance with applicable laws, rules, regulations, and policies pertaining to the management and retention of City records.
- 4.1.10. Misrepresenting, obscuring, suppressing, or replacing a *User's* identity on an electronic communications system is forbidden. The *User* name, *Electronic Mail*

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 6 of 12 |
| | Effective Date May 5, 2017 | | |

address, and related information used for login/access and included with messages or online postings must reflect the actual originator of the messages or postings.

- 4.1.11. *Users* shall not download or store software from the *Internet* on *City Computer Equipment* which has not been properly licensed to the City or in which the City does not have a legal right to possess or use. *Users shall not install unauthorized or unlicensed software programs on City Computer Equipment. Any authorization must be obtained in advance from the Department of IT.*
- 4.1.12. An *Information Security* Committee or its successor, as defined and chartered through the City's IT governance structure, will meet periodically to review the current status of the City's *Information Security*, review and monitor security incidents within the City, approve and periodically review *Information Security* projects, and provide semi-annual reports related to these activities to the Dept. of IT.
- a. The *Information Security* Committee will review this policy and the related *Information Security Standards and Guidelines* annually during the first quarter of each fiscal year, making recommendations for any updates to the Dept. of IT. The Dept. of IT will forward any recommended updates to the City executive management team for approval.

4.2. Departmental Management Policy

- 4.2.1. Department Directors are ultimately responsible for departmental compliance with the provisions of this policy and other *information security* and acceptable use policies.
- 4.2.2. Senior management will lead by example by ensuring *Information Security* is given a high priority in all current and future business activities and initiatives.
- 4.2.3. Management must provide all *Users* within their department with sufficient training to allow them to understand their personal responsibilities to properly protect information resources, including tracking of the dates and names of employees trained. *Information Security* training materials will be created, maintained, and made available by the Dept. of IT. Such training should occur within the first 90 days of employment, and then refresher training should occur annually for all employees.
- 4.2.4. Management must allocate sufficient on-the-job time for *Users* to acquaint themselves with *Information Security Policies*, separately from the formal training required in Section 5.3 above, including the *Information Security Standards and Guidelines* with related procedures on prohibited activities and

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 7 of 12 |
| | Effective Date May 5, 2017 | | |

appropriate ways to report security threats. Management must notify *Users* of specific actions that constitute security violations and that such violations will be logged.

- 4.2.5. Each department will designate an *Information Security Liaison* (ISL) to be the primary point of contact responsible for department compliance with the City's *Information Security Policies* and coordination with the Dept. of IT. The *Information Security Liaison* should be a senior IT staff member or unclassified manager. The City's Chief *Information Security Officer* will manage the ISL program and provide information and training pertinent to the position to assist in protecting City IT assets.
- 4.2.6. Each department will review their own security practices at least annually for conformance with this policy and compliance with the *Information Security Standards and Guidelines*.
- 4.2.7. All department and City *Computer Systems* privileges must be promptly terminated at the time a *User* leaves City employment or ceases to provide services to or receive services from the department or the City. Such termination of access to City *Computer Systems* includes revocation of the assigned *User ID* and must occur as soon as possible and, in any case, no more than three (3) business days, after access is no longer required. All files held in the *User's* home directory, as applicable, will be held for 90 days for their supervisor or designee to review and will then be deleted. All City records shall be retained in accordance with the department's approved Records Disposition Schedule or the Citywide General Records Disposition Schedule
- 4.2.8. Records reflecting the *Computer Systems* on which *Users* have accounts must be kept up-to-date and reviewed periodically, at least annually, by the respective Department Head or designee, so *Computer Systems* access privileges may be expeditiously revoked on short notice, if the need arises.
- 4.2.9. To provide evidence for investigation, prosecution or disciplinary actions, relevant *Computer Systems* information should be immediately captured and preserved whenever it is suspected that a computer *Breach*, crime or abuse has taken place. The relevant information must be securely stored offline until such time as legal counsel determines the City will no longer need the information. The information to be immediately collected shall include the current system status and backup copies of all potentially involved files. The *Information Security Liaison* or *User* who discovers the suspected *Breach*, crime or abuse should report such to the Dept. of IT, Chief *Information Security Officer* who will take action to preserve the relevant information.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 8 of 12 |
| | Effective Date May 5, 2017 | | |

- 4.2.10. To ensure a quick, effective, and orderly response to *information security* incidents, the *Information Security* Committee will identify a “Cyber Security Incident Response Team” (CSIRT) comprised of IT staff to handle the reporting of and response to *information security* incidents. The reporting of incidents will be done according to the *Information Security Standards and Guidelines*.
- 4.2.11. All known vulnerabilities of the City’s *Computer Systems*, in addition to suspected or known violations, must be communicated in an expeditious and confidential manner to the Dept. of IT, the Chief *Information Security* Officer, the IT Service Provider, and any others designated by the Dept. of IT.
- 4.2.12. Except as specifically provided for in this policy, other *Information Security Policies* and procedures or otherwise provided by law, reporting *information security* violations, problems or vulnerabilities to any person outside the City, except to an appropriate government or law enforcement agency, without the prior written approval of the Dept. of IT, is strictly prohibited.
- 4.2.13. Criticality levels will be assigned to each business application to reflect the potential impacts resulting from a *Breach*, data corruption or denial of service. No less than once every two years, the Dept. of IT will conduct a rating survey to inventory and assign criticality levels to City applications. Each Department Director or their designee will assign criticality levels and data elements based on criteria established by the *Information Security* Committee. The Dept. of IT will maintain a master list of all inventoried applications and assigned ratings.

4.3. *User Policy*

- 4.3.1. *Users* must be responsible in their use of City *Computer Equipment*, and *Network Services*. Any action that may cause interference with City *Computer Systems* exposes the City’s *Computer Systems* to risk or adversely impacts the work of others in using these *Computer Systems* is prohibited.
- 4.3.2. Employees may be disciplined in accordance with standard City procedures for improperly using or knowingly allowing the improper use of the City’s *Computer*
- 4.3.3. *Equipment*, *Network Services* or *Email* system as stated in this regulation. Abuse of the City’s *Computer Systems* may result in disciplinary action, up to and including termination and criminal prosecution if deemed appropriate.
- 4.3.4. Employees should cooperate fully with all investigations, regarding the abuse of the City’s *Network Services*, *Computer Equipment*, *Computer Systems*, and the *Internet*.
- 4.3.5. Every end *User* must have a single unique *User ID* and a personal password which must be kept confidential and not shared with anyone else. This *User ID* and

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|-----------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 9 of 12 |
| | Effective Date May 5, 2017 | | |

password will be required for access to all multi-user *Computer Equipment* and *Network Services*. *User* passwords must comply with the *Information Security Standards and Guidelines*.

- 4.3.6. *Users* accessing City *Computer Systems* are prohibited from gaining unauthorized access to any other non-City *computer systems* or in any way damaging, altering or disrupting the operations of those systems. *Users* are also prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.
- 4.3.7. Employees who use City *Computer Systems*, *Computer Equipment*, *Network Services*, or the City's *Email* shall sign an *Information Security Policy Acknowledgement Form* which states that the employee agrees to comply with the terms of this Administrative Regulation.

4.4. System Manager/Administrator Policy

- 4.4.1. Every multi-user system must include sufficient automated tools to assist *System Managers* in verifying the security status of the *Computer Equipment* and *Computer Systems*. These tools must include mechanisms for automated notifications to be sent to *System Managers* and for the correction of security problems.
- 4.4.2. Whenever a City *Computer System* has been *Breached* by an unauthorized party, or there is a reasonable suspicion of a *Breach* or other system compromise, *System Managers* must immediately change the password on the involved system and any other systems at risk from the *Breached* account. Under either of these circumstances, all recent changes to *User* and system privileges must be reviewed for unauthorized modifications.
- 4.4.3. Production application systems which access financial or sensitive information must generate logs that show every addition, modification, and deletion to such information.
- 4.4.4. Mechanisms used to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software or the logs themselves
- 4.4.5. All *Computer Systems* and application logs must be maintained in an environment where they cannot readily be viewed by unauthorized persons. By definition, a person is unauthorized if he or she is not a member of the authorized network security group(s) which allow access to such logs.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|------------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 10 of 12 |
| | Effective Date May 5, 2017 | | |

- 4.4.6. Logs of computer security related events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, security measures. Logs containing computer security related events must be retained in accordance with the applicable department's Records Disposition Schedules or the Citywide General Records Disposition Schedule. During this period, the logs must be secured so that they cannot be modified, and so that they can be read only by authorized persons. These logs are important for error correction, forensic auditing, security *Breach* recovery, and related efforts.
- 4.4.7. To allow proper remedial action, *System Managers* must, on a daily basis, review records reflecting security relevant events on multi-user machines/systems.
- 4.4.8. When a person who is authorized as a System Manager or System Administrator ceases to perform those functions, then such person's access to City *Computer Systems*, *Computer Equipment*, *Network Services*, and applications must be immediately revoked and system-level passwords to which he or she had access must be changed as soon as possible and, in any case, no more than twenty-four (24) hours after such System Manager or System Administrator ceases to perform those functions. In addition, such person's physical access to City *Computer Systems*, *Computer Equipment*, and *Network Services* must be restricted or revoked immediately, as appropriate.

5. RESPONSIBILITY

5.1. Mayor

- 5.1.1. The Mayor will establish regulations and procedures regarding the security and safeguarding of City data, *Computer Equipment*, *Computer Systems*, and *Network Services*.

5.2. Chief Information Officer

- 5.2.1. The Chief Information Officer has the responsibility to provide *Guidelines*, strategic direction, oversight, and coordination of citywide *Computer Systems*.

5.3. Chief *Information Security* Officer

- 5.3.1. The Chief *Information Security* Officer or designee will direct and manage the planning and supervision of all *Information Security* services for the City, including those provided by vendors/providers.

5.4. Strategic Technology Advisory Committee (STAC)

- 5.4.1. The Strategic Technology Advisory Committee (STAC) or other IT governing

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|------------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 11 of 12 |
| | Effective Date May 5, 2017 | | |

body as assigned by the City Chief Operating Officer is responsible for approving *Information Security Standards and Guidelines*.

5.5. *Information Security Committee*

5.5.1. The *Information Security Committee* or other IT governing body as assigned by the STAC is responsible for reviewing departments' initial requests for exemptions from the *Information Security Standards and Guidelines* and recommending modifications to the City's existing *Information Security Standards and Guidelines*, as necessary

5.6. IT Services Provider(s)

5.6.1. The City's IT services provider(s) will be responsible for providing, operating, and maintaining the City's primary *Computer Systems*, and *Email* systems, *Network Services*, and *Internet* connectivity. The IT services provider is charged with the responsibility of protecting the City's *Network Services* and *Computer Systems* from intrusion from outside sources, including the management and maintenance of firewalls

5.7. Department Directors

5.7.1. Department Directors or their designees are responsible for approving requests for *User IDs* and *User Accounts* for *Email* and *Network Services*.

5.8. *Information Security Liaison*

5.8.1. The departmental *Information Security Liaison* is the primary point of contact responsible for department compliance with the City's *Information Security Policies*.

5.9. System Administrators and System Managers

5.9.1. *System Administrators* and *System Managers* are responsible for maintaining the security and integrity of City *Computer Systems* and *Network Services*, including duties related to creating, modifying, and deleting *User IDs* or *User Accounts*, and for maintaining the confidentiality of data contained on those systems in compliance with the City's *Information Security Policies*.

5.10. IT Asset Manager

5.10.1. The department IT Asset Manager is responsible for maintaining an accurate, up-to-date inventory of all departmental IT assets, including computer hardware and software.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|-------------------------------|------------|------------------|
| SUBJECT INFORMATION SECURITY POLICY | Number 90.63 | Issue 2 | Page 12 of 12 |
| | Effective Date May 5, 2017 | | |

5.11. Supervisory Personnel

5.11.1. Supervisory Personnel are responsible for overseeing the employee's use of City *Computer Systems, Email systems, and Network Services.*

5.12. Every Individual is responsible for his/her actions and conduct in accessing or using the City's *Computer Systems, Network Services, and Email Systems.* Violation of the City's *Information Security Policies* or unauthorized or inappropriate use may result in disciplinary action.

APPENDIX

Legal References

San Diego Municipal Code, section 27.3564(b)

Administrative Regulation 45.50 - Private Use of City Labor, Equipment, Materials, and Supplies Prohibited

Administrative Regulation 90.20 - Office Telephones

Administrative Regulation 90.62 - Information and Communications Technology Acceptable Use

Administrative Regulation 90.64 - Protection of Sensitive Information and Data

Administrative Regulation 90.65 - Broadcast Email and Voice Mail

Forms Involved

Employee Acknowledgement of IT Security Policy Overview

Form IT-063 - Information Security Policy Acknowledgement

Subject Index

Computer Equipment, Security Computer Systems, Security

Electronic Mail, Security Email, Security

Internet, Security

Network Services, Security

Security – Information Technology

Distribution

All Departments (Mayoral and Non-Mayoral)

Administering Department

Department of IT

Information Security Policy Acknowledgement Form – City Employees

Policy Summary (pertinent excerpts from Administrative Regulation 90.63):

4.1.2. All computer files developed, created or enhanced within the scope and course of City employment, or a City third-party contractual relationship, are the property of the City of San Diego, regardless of their physical location or the form in which they are maintained. These include, but are not limited to, computer data files, documents, databases, spreadsheets, calendar entries, appointments, tasks, and notes which reside on any City Computer Systems or Computer Equipment, or the Computer Equipment of a contractor performing work for or on behalf of the City.

a. The City reserves the right to access and disclose as required or permitted by law, and as defined in the approved Information Security Standards and Guidelines, all messages and other electronic data sent over its Email systems or stored in computer files on City Computer Equipment. City-related computer files stored on non-City or personal computers must be provided upon the City's request in City standard formats.

4.1.4. Authorized access to City Computer Systems and Network Services shall be at the minimum level required for the Individual to perform and complete their assigned duties, and not at a level that allows access to information beyond the scope of that Individual's assigned duties.

4.1.5. Each Computer System or Network Services User ID must uniquely identify only one User. Generic, shared, or group User IDs are not permitted. [...] Network security groups may be used to combine Users access rights. Approved group Email accounts may be shared by multiple Users who each have unique User IDs.

4.3.1. Users must be responsible in their use of City Computer Equipment, and Network Services. Any action that may cause interference with City Computer Systems, exposes the City's Computer Systems to risk or adversely impacts the work of others in using these Computer Systems is prohibited.

4.3.2. Employees may be disciplined in accordance with standard City procedures for improperly using or knowingly allowing the improper use of the City's Computer Equipment, Network Services or Email system as stated in this regulation. Abuse of the City's Computer Systems may result in disciplinary action, up to and including termination and criminal prosecution if deemed appropriate.

4.3.4. Every end User must have a single unique User ID and a personal password which must be kept confidential and not shared with anyone else. This User ID and password will be required for access to all multi-user Computer Equipment and Network Services. User passwords must comply with the Information Security Standards and Guidelines.

4.3.5. Users accessing City Computer Systems are prohibited from gaining unauthorized access to any other non-City Computer Systems or in any way damaging, altering or disrupting the operations of those systems. Users are also prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.

Employee/Supervisor Acknowledgement

By signing below, the employee acknowledges that he or she has been advised of the City's policies related to Information Security as provided in Administrative Regulation 90.63 ("Information Security Policy"), which has been discussed with his or her supervisor, and further acknowledges that he or she understands and agrees to comply with the provisions of the policy. Employee understands that this form will be kept as part of his or her departmental employee file, and that he or she may receive a copy, if requested. The supervisor acknowledges that he or she has discussed the policy (A.R. 90.63) with the employee named below and understands the supervisor's obligations regarding Information Security under this policy.

Employee's Name (Print Legibly)

Employee's Signature

Date Signed

Supervisor's Name (Print Legibly)

Supervisor's Signature

Date Signed

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|------------------------------------|------------|----------------|
| SUBJECT INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE | Number 90.62 | Issue 2 | Page 1 of 7 |
| | Effective Date December 7, 2012 | | |

1. PURPOSE

- 1.1 This regulation defines acceptable uses of the City's information and communications technology resources.
- 1.2 This regulation also defines unacceptable actions and uses of City information and communications technology resources.
- 1.3 The standards set forth in this regulation are minimum standards for City Departments. Departments may develop rules and procedures regarding department-specific use of information and communications technology resources in order to implement this policy. Departments may also develop more restrictive rules for the particular department, when required to comply with local, state or federal laws or regulations.

2. SCOPE

- 2.1 This regulation applies to all information and communications technology resources owned or leased by the City, or that are provided as a service to the City, including future emerging technologies that may be implemented, and activities using any City-paid accounts, subscriptions or other technology services, such as Internet and World Wide Web access, voice mail, and Email, regardless of where the activities are conducted.
- 2.2 This regulation applies to all City employees, volunteers, and other City agents, collectively referred to as "Individuals," using some or all of the City's Information and Communications Technology Resources.
- 2.3 The City's information and communications technologies are provided for the benefit of City Departments in providing public services.

3. DEFINITIONS

- 3.1 "IT" – Information Technology

(Supersedes Administrative Regulation 90.62, Issue 1, effective October 1, 1996)

Authorized



MAYOR


PERSONNEL DIRECTOR


CITY CLERK


CITY ATTORNEY


INDEPENDENT BUDGET
ANALYST


CITY AUDITOR

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|------------------------------------|------------|----------------|
| SUBJECT | Number 90.62 | Issue 2 | Page 2 of 7 |
| INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE | Effective Date December 7, 2012 | | |

- 3.2 “FTP” – File Transfer Protocol – A protocol used to transfer files between networked devices.
- 3.3 “Email” (Electronic Mail) – The electronic transfer of information typically in the form of electronic messages, memoranda, notes, meeting appointments, and attached documents from a sender to one or more recipients via a telecommunications network.
- 3.4 “Information and Communications Technology Resources” or “City IT Resources” – All technology resources owned or leased by the City and any City-paid accounts, subscriptions or other technology services. This includes office telephones, wireless/cellular telephones, smart phones, desktop and portable computer systems, printers fax machines, Internet and World Wide Web (Web) access, internal and external Email, electronic bulletin boards or newsgroups, file transfer protocol (FTP), other wireless systems, and emerging communications systems or devices.
- 3.5 “Internet” - is a network of networks connecting computer systems throughout the world. In addition to providing capability for Email, other Internet applications include, but are not limited to, news groups, FTP, telnet and the Web.
- 3.6 “Confidential” - For the purpose of this Administrative Regulation, confidential information refers to City information not authorized or intended to be disclosed outside the City. Such information shall only be accessible or disclosed to those individuals who have a business need to know, and shall not otherwise be disclosed unless disclosure is required by contract, ordered by a court, or required under applicable local, state, or federal laws or regulations. Confidential is not intended to cover City sensitive data category which is governed by state and federal law (e.g. social security numbers, credit card numbers, medical record information and etc.). Refer to AR90.64 for the Sensitive Data Administrative Regulation.

4. GENERAL POLICY

- 4.1 Use of City IT Resources shall be limited to work-related, City business purposes only. Personal files should not to be stored on City equipment.
- 4.2 When using the City's Email system, the Internet or other City IT Resources to communicate with others external to the City organization, individuals are representing the City of San Diego and therefore must communicate in a business-like manner. Refer to “Best Practices and Tips” on the CityNet site (located at Departments – Human Resources – Resources and Tools - Customer Service Best Practices and Tips) to ensure the communication is not in conflict with City policies or regulations.
- 4.3 The City's IT Resources and the data stored on them are the property of the City. An individual has no right of privacy in any information or data maintained in or on City IT

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|------------------------------------|------------|----------------|
| SUBJECT | Number 90.62 | Issue 2 | Page 3 of 7 |
| INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE | Effective Date December 7, 2012 | | |

resources. Access to City IT Resources is a privilege which can be revoked at any time at the discretion of City management.

- 4.4 If during the course of employment, an individual performs or transmits work using City IT Resources, that work may be subject to the investigation, search, and review of others in accordance with this or other policies.
- 4.5 Unacceptable Uses: Notwithstanding any provisions of law to the contrary, the following uses of City IT Resources are expressly prohibited. This list does not necessarily include all possible unacceptable uses and may be expanded as new technologies emerge. The City retains the right to sanction individuals, as deemed appropriate, for unacceptable uses that may be defined later. Where a prohibited use is defined as "unauthorized" below, proper authorization must be requested in writing, in advance, through the Department of Information Technology or as otherwise directed.
- 4.5.1 Use of City telephones (landlines or wireless) for personal long distance calls. Such calls should be made through the use of a personal telephone credit card or with operator assistance and billed to the caller's home telephone number.
- 4.5.2 Illegal activities including but not limited to fraud, theft, copyright infringement.
- 4.5.3 Use for personal profit, including the conducting of private commercial activities, solicitation or other personal business interest, or for the profit of another organization.
- 4.5.4 To conduct political activities as described by San Diego City Charter section 31 or San Diego Municipal Code section 27.3564(b).
- 4.5.5 To play online games or gamble.
- 4.5.6 To knowingly send, save, view or access material containing content that may be considered offensive to a reasonable person. Offensive material includes, but is not limited to, pornography, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend someone on the basis of his or her race, color, creed, sex, age, national origin or ancestry, physical or mental disability, veteran status, marital status, medical condition, sexual orientation, and any other category protected by federal, state, or local laws. Any use of City IT Resources to harass, threaten or discriminate is strictly prohibited by the City.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|------------------------------------|------------|----------------|
| SUBJECT INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE | Number 90.62 | Issue 2 | Page 4 of 7 |
| | Effective Date December 7, 2012 | | |

- 4.5.7 To knowingly send, save, view or access material containing content that may reasonably be considered threatening to any individual.
- 4.5.8 Actions or attempted actions to bypass, defeat or attack established City network, server, computer or any other security controls.
- 4.5.9 Unauthorized addition or modification to the City network, which includes, but is not limited to, the connection of personal or unauthorized network switches, routers, and wireless access points.
- 4.5.10 To read, delete, copy or modify Email of other users, without appropriate delegation or advanced authorization.
- 4.5.11 Any actions for the purpose of hacking, tampering, trespassing, probing, eavesdropping, monitoring, wiretapping, cracking, recording, breaching, surveying, intercepting, data theft, forgery, sabotage, spoofing (forgery of digital identity) of electronic communications and excessive loading or congesting (i.e., Denial of Service attack) of the City network or computers. This prohibition does not apply to legitimate investigations conducted by authorized persons or agencies in the collection of evidence.
- 4.5.12 To access or modify data or programs for which a user does not have authorization or explicit consent from the owner of the data/information, or from an appropriate level of management. (Refer to A.R. 90.64)
- 4.5.13 To knowingly introduce, distribute, propagate or download any computer viruses or other contaminants (e.g., computer worms or Trojans).
- 4.5.14 Accessing streaming audio or video or any other bandwidth intensive activities from Internet resources at any time for non-business use. Exceptions include streaming video from City of San Diego "City TV" as "City TV" is considered to be a work-related activity, and emerging technologies that may be used for City-related activities (e.g., posting of City communications on social media websites).
- 4.5.15 To download any software or applications from the Internet for personal use at any time, or for business use without proper advance approval from department management and the Department of IT.
- 4.5.16 To send or attempt to send "spam" messages (unsolicited Email messages, usually to a large number of recipients, including the sending of junk mail or other advertising material to individuals who did not specifically request such material), junk mail or any other for-profit messages, "chain letters" or any

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|------------------------------------|------------|----------------|
| SUBJECT INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE | Number 90.62 | Issue 2 | Page 5 of 7 |
| | Effective Date December 7, 2012 | | |

other mass mailings of a non-work related nature. (Refer to Administrative Regulation 90.65)

- 4.5.17 To forward Email or upload any file attachments containing confidential City data or information to a personal (external) Email account (e.g., Yahoo, AOL, etc.).
- 4.6 Individuals shall not disclose any of the City's internal (i.e. proprietary or confidential) operations information on external (public or private) web logs ("blogs"), chat rooms, Internet forums, message boards, social media sites (Facebook, Twitter or YouTube) or other publicly accessible web sites, without the prior, written authorization from City management or City Council as required by policy or law. This does not apply to any information that is already publicly available from the City's web site or other sites where the information was authorized to be posted.
- 4.7 The Department of IT is responsible for the development and management of the City's public Web Site (www.sandiego.gov) and the City's internal CityNet Web Site (citynet.sannet.gov). The Department of IT is the final authority for approving content from departments to ensure compliance with City Web Site guidelines and standards for appropriateness, style, structure, functionality, and accessibility, including compliance with the Americans with Disabilities Act.
- 4.8 City Departments shall use the City's official public Web Site for all official City Internet postings. Social Media may only be used in accordance with the Social Media Guidelines available on Citynet (Located at Departments - Department of Information Technology – IT Services – Web Services – Web Policies & Procedures).
- 4.9 New Web Sites or Internet Domain Names shall not be obtained or created without the prior written approval of the Department of IT.

5. EMAIL POLICY

- 5.1 Email, and the electronic distribution of documents, is subject to all the same laws, policies and practices that apply to other means of communication, such as telephone and paper documents and records. This includes, but is not limited to, product endorsements, copyright laws, software licensing, patent laws, record retention, and proper business correspondence practices.
- 5.1.1 Transmission of any material in violation of Local, State or Federal laws or regulations and City policy and procedures is prohibited.
- 5.1.2 Under the California Public Records Act, any Email may be a public record. Individuals should be aware that electronic records are subject to the mandatory

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|------------------------------------|------------|----------------|
| SUBJECT | Number 90.62 | Issue 2 | Page 6 of 7 |
| INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE | Effective Date December 7, 2012 | | |

public disclosure requirements of the Public Records Act, and subject to exceptions under the Act. Public Records Act requests should be handled in accordance with the City policy direction as stated in A.R. 95.20.

- 5.2 Individuals are responsible for all Email messages and attached documents originating from his/her user Email address and for directing Email only to intended recipients.

6. EMPLOYEE AND SUPERVISOR RESPONSIBILITIES

- 6.1 City IT Resources are provided for use in the pursuit of City business and are to be reviewed, monitored, and used only in that pursuit.
- 6.2 Each Individual is responsible for the content of all text, audio, or images that they place or send using City IT Resources.
- 6.3 Individuals who misuse City IT Resources are subject to disciplinary action up to and including termination.
- 6.4 The City may advise appropriate legal officials of any evidence of illegal activities. Individuals should contact their supervisor if they have any questions regarding appropriate use of City IT Resources.
- 6.5 Individuals accessing computers on the City network must acknowledge Acceptable Use prior to accessing City computers. City computers will prompt users for this acknowledgement prior to allowing access to the system.
- 6.6 Email and Internet/Web access are not entirely secure. Others outside the City may also be able to monitor Email and Internet/Web access. For example, Internet sites maintain logs of visits from users; these logs identify which particular person (based on Internet Protocol (IP) address) accessed the service. If an Individual's work requires a higher level of security, contact departmental IT staff or the Department of IT for guidance on securely exchanging Email or gathering secure information from sources such as the Internet or World Wide Web.
- 6.7 Individuals should safeguard the City's confidential information, as well as that of customers and others, from disclosure. Messages should be screened for confidential information prior to being viewed or shared with others. Messages containing confidential information should not be left visible while an individual is away from his or her work area. Department Directors should be engaged to provide guidance on confidential information and what security controls, if any, need to be applied to the information prior to being sent over Email.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|------------------------------------|------------|----------------|
| SUBJECT | Number 90.62 | Issue 2 | Page 7 of 7 |
| INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE | Effective Date December 7, 2012 | | |

APPENDIX

Legal References

San Diego City Charter Section 31

San Diego City Municipal Code Section 27.3654(b)

San Diego Administrative Regulation (AR) 45.50, "Private Use of City Labor, Equipment, Materials, and Supplies Prohibited"

AR 90.20, "Office and Wireless Telephones"

AR 90.63 "Information Security Policy"

AR 90.64, "Protection of Sensitive Information and Data"

AR 90.65, "Broadcast Email and Voice Mail"

AR 95.05, "Cell Phone and Other Handheld Communication Device Use Policy"

Subject Index

Information Technology

Acceptable Use – Information Technology & Communications

City Web Site, Acceptable Use

Computer Equipment, Acceptable Use

Communications Systems, Acceptable Use

Electronic Mail, Acceptable Use

Email, Acceptable Use

Network Services, Acceptable Use

Distribution

Department Heads

Department IT Administrators & Analysts

System Administrators

Administering Department

Department of Information Technology

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|--------------------------------|------------|----------------|
| SUBJECT CONFLICT OF INTEREST AND EMPLOYEE CONDUCT | Number 95.60 | Issue 2 | Page 1 of 8 |
| | Effective Date May 23, 1990 | | |

1. PURPOSE

1.1 The purpose of this regulation is to:

- a. Summarize in a single document a code of ethics and acceptable employee conduct which will apply equally to all employees, regardless of individual job duties and responsibilities.
- b. Emphasize that each employee in our city occupies a position of public trust which demands the highest moral and ethical standard of conduct.
- c. Ensure that citizens are given efficient, productive, and high quality services in a courteous impartial manner. Such services should be equally available, with no special advantage given any citizen beyond that available to all citizens.

1.2 Policies and regulations governing the conduct of City employees appear in the California Government Code, City Charter, Municipal Code, Council Policy Manual, Administrative Regulations, Personnel Manual, and Departmental Instructions. Employees shall familiarize themselves with the pertinent sections of these documents and consult them as necessary for information and guidance.

2. SCOPE

2.1 This regulation applies to all City of San Diego Employees.

(Supersedes Administrative Regulation 95.60, Issue 1, effective March 27, 1970)

Authorized

(Signed by John Lockwood)

CITY MANAGER

(Signed by John W. Witt)

CITY ATTORNEY

(Signed by Rich Snapper)

PERSONNEL DIRECTOR

(Signed by Charles G. Abdelnour)

CITY CLERK

(Signed by Judith Bauer)

INTERGOVERNMENTAL RELATIONS DIRECTOR

(Signed by Ed Ryan)

AUDITOR & COMPTROLLER

(Signed by Bob Spaulding)

PLANNING DIRECTOR

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|--------------------------------|------------|----------------|
| SUBJECT CONFLICT OF INTEREST AND EMPLOYEE CONDUCT | Number 95.60 | Issue 2 | Page 2 of 8 |
| | Effective Date May 23, 1990 | | |

3. POLICY

3.1 Responsibility of Ethical Conduct

It is the responsibility of all City of San Diego employees to engage in ethical behavior and practices. Every employee is responsible for both the actual and perceived conflict of interest that may arise as a result of the employee's actions and it is the employee's responsibility to reduce or eliminate to the extent possible such actual and perceived conflicts of interest.

3.2 Responsibility of Public Services

All City of San Diego employees are bound to uphold the Constitution of the United States and the Constitution of the State of California, and to abide by the laws of the nation, state, and the City. They are bound to observe in their official acts, the highest standards of integrity and to discharge faithfully the duties of their position, recognizing that the lives, safety, health and welfare of the general public must be their primary concern. Their conduct in both their official and private affairs should be above reproach to assure that their public position is not used nor perceived as being used for personal gain. The conduct of all employees shall be such as to provide the best public service to each citizen and the community as a whole. The conduct of all employees shall be consistent with the goals and values of this organization.

3.3 General Rule Regarding Conflict of Interest

Employees shall not engage in any business or transaction, and shall not have a financial or other personal interest, direct or indirect, which is incompatible with the proper discharge of their official duties or would tend to impair their independence, judgment, or action in the performance of such duties.

3.4 Acceptance of Favors, Gifts, and Gratuities

Persons in the public service shall not accept money or other consideration or favors from anyone other than the City for the performance of an act which they would be required or expected to perform in the regular course of their duties. This prohibition would not normally include items such as plaques, souvenirs, or mementos of nominal value often associated with a given event. Persons shall not accept gifts, gratuities or favors of any kind which might reasonable be interpreted as an attempt to influence their actions with respect to City business.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|--------------------------------|------------|----------------|
| SUBJECT CONFLICT OF INTEREST AND EMPLOYEE CONDUCT | Number 95.60 | Issue 2 | Page 3 of 8 |
| | Effective Date May 23, 1990 | | |

3.5 Collateral or Outside Employment

a) Notification and Departmental Approval

Persons employed with the City who are engaged in any collateral or outside business activity or employment shall notify the Department Director or other appropriate appointing authority in writing. Persons contemplating such business activity or employment shall obtain departmental approval before accepting such employment.

b) General Prohibition

Pursuant to Council Policy 000-4, employees shall not engage in any collateral employment or business activity which is incompatible or in conflict with the duties, functions, or responsibilities of the City, the appointing authority, the department, or the employee. Activities which may constitute a conflict include: use of their City time, facilities, equipment and supplies, or the use of a badge, uniform, prestige or influence of their City or employment for private gain or advantage. An employee shall not engage in any collateral business activity or employment, which, by its nature, hours or physical demands, would impair the required quality or quantity of the employee's work with the City, impair the employee's independence of judgment or action in the performance of official duties, reduce the effectiveness or efficiency of the employee's department, reflect discredit on the City, or tend to increase the City's payments for Sick Leave, Worker's Compensation benefits, Long Term Disability or Industrial Leave benefits.

c. Specific Prohibitions

- 1) Employees shall not work within their discipline or profession for a company or as a self-employed consultant when their work is reviewed, or approved, or is subject to issuance of a permit by their City department.
- 2) Employees shall not submit work they have done for a collateral employer or as a self-employed consultant to the employee's division in the City for review, approval, or issuance of a permit.
- 3) Employees shall not review, approve, or issue a permit for work done by a collateral employer, whether the work submitted was done by the City employee or other staff of the collateral employer.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|--------------------------------|------------|----------------|
| SUBJECT CONFLICT OF INTEREST AND EMPLOYEE CONDUCT | Number 95.60 | Issue 2 | Page 4 of 8 |
| | Effective Date May 23, 1990 | | |

- 4) Employees shall not attempt to influence the City's review, approval, or issuance of a permit pertaining to work submitted by an employee's collateral employer, whether the work submitted was done by the City's employee or other staff of the collateral employer.
- 5) Employees in supervisory positions shall not assign to a subordinate any work a) resulting from the supervisor's collateral employment, and b) requiring the City's review, approval, or issuance of a permit.
- 6) Employees in supervisory positions shall not attempt to influence the City's review, approval, or issuance of a permit pertaining to any work resulting from the supervisor's collateral employment.

3.6 Use of City Employment and Facilities for Private Gain

Persons in the public service shall not use, for private gain or advantage, their City time or the City's facilities, equipment or supplies. In addition, City employees shall not use or attempt to use their position to secure unwarranted privileges or exemptions for themselves or others. Administration Regulation 45.50, "Private Use of City Labor, Equipment, Materials, and Supplies Prohibited" is incorporated by reference in this paragraph.

3.7 Use of Confidential Information

Persons in the public service shall not use confidential information acquired by or available to them in the course of their employment with the City for speculation or personal gain. Persons in the public service shall uphold the public's right to know, and in accordance with the Ralph M. Brown Act, uphold the public's right to know not only the decisions taken, but also the deliberations which shape public policies.

Persons in the public service shall not disclose confidential personnel information acquired by or available to them in the course of their employment with the City except in the performance of their duties as required by law.

3.8 City Contracts

In accordance with Government Code section 87100 et. seq. and Government Code section 1090 et seq., persons in the public service shall not exercise any discretionary powers for, or make recommendations on behalf of the City or department or officer thereof with respect to any contract or sale to which the City or any department thereof is a party and in which such persons shall knowingly be directly or indirectly financially interested.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|--------------------------------|------------|----------------|
| SUBJECT CONFLICT OF INTEREST AND EMPLOYEE CONDUCT | Number 95.60 | Issue 2 | Page 5 of 8 |
| | Effective Date May 23, 1990 | | |

3.9 Personal Investments

In accordance with Government Code section 87100 et seq., persons in the public service shall not make personal investments in enterprises which they have reason to believe may be involved in decisions or recommendations to be made by them, or under their supervision, or which will otherwise create conflict between their private interests and the public interest. If, however, persons in the have financial interests in matters or enterprises coming before them, or before the department in which they are employed, they shall disqualify themselves from any participation therein.

3.10 Discussion of Future Employment

Persons in the public service shall not negotiate for future employment outside the City service with any person, firm, or organization known by such persons to be dealing with the City concerning matters within such person's areas of responsibility or upon which they must act or make a recommendation, when the person's City employment status could create an advantage not available to other individuals, firms or organizations. City employees shall not communicate with former City employees on any issue or matter in which that former employee had official responsibility or participation for a period of one year from the former employee's final date of active employment. Council Policy 300-11, "City Contract Provisions with Respect to Hiring City Employees" is incorporated by reference in this paragraph.

3.11 Equal Employment

Persons in the public service shall not, in the performance of their service responsibilities, discriminate against any person on the basis of race, religion, color, creed, age, marital status, national origin, ancestry, sex, sexual preference, medical condition, or handicap and they shall cooperate in achieving the equal employment opportunity and affirmative action goals and objectives of the City.

3.12 Reporting of Improper Government Activities

Persons in the City service are strongly encouraged to fulfill their own moral obligations to the City by disclosing to the extent not expressly prohibited by law, improper governmental activities within their knowledge. Employees are encouraged to contact departmental management with this information.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|--------------------------------|------------|----------------|
| SUBJECT CONFLICT OF INTEREST AND EMPLOYEE CONDUCT | Number 95.60 | Issue 2 | Page 6 of 8 |
| | Effective Date May 23, 1990 | | |

No officer or employee of the City shall directly or indirectly use or attempt to use the authority or influence of such officer or employee for the purpose of intimidating, threatening, coercing, commanding, or influencing any person with the intent of interfering with that person's duty to disclose such improper activity.

3.13 Favoritism

Supervisory or management employees shall not participate in the appointment or recommend the appointment of any member of their immediate family, or any other person with whom the employee has a close personal or private business relationship, to a classified position of any department, office, bureau or division over which they have administrative control.

Supervisory or management employees shall not participate in the appointment or recommend the appointment of a member of their immediate family, or any other person with whom the employee has a close personal or business relationship, to another supervisory or management position of the City. This regulation permits immediate family members and close personal friends of supervisory or management employees to be appointed as classified employees in any department provided such supervisory or management employees make no recommendation nor otherwise attempt to influence such appointments.

No supervisory or management employee shall: 1) directly supervise any immediate family member or person with whom the supervisor has a close personal relationship (this does not apply to OCA assignments of 30 days or less); 2) influence the approval of any employee rewards for any immediate family member or person with whom the supervisor has a close personal relationship; 3) interfere with any performance evaluation or disciplinary proceeding for any immediate family member or person with whom the supervisor has a close personal or business relationship; and 4) recommend or attempt to influence any contractor or business which has a business relationship with the City to employ a member of his or her immediate family or any other person with whom the employee has a close personal or business relationship.

For purposes of this section, the term "immediate family" shall mean spouse, significant other, son, daughter, mother, father, brother, brother-in-law, sister, sister-in-law, mother-in-law, father-in-law, aunt, uncle, niece, nephew, step-parent, step-child.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|--------------------------------|------------|----------------|
| SUBJECT CONFLICT OF INTEREST AND EMPLOYEE CONDUCT | Number 95.60 | Issue 2 | Page 7 of 8 |
| | Effective Date May 23, 1990 | | |

3.14 Product Endorsement

City employees, in their capacity as a City employee, shall not endorse a product or service or comment on that product or service if it is the intent of the solicitor of the endorsement, or of the vendor or manufacturer of that product or service, to use such comments for purposes of advertisement. City employees are not prohibited from responding to inquiries regarding the effectiveness of products or services used by the City unless the employee is aware that it is the inquirer's intention to use those comments for purpose of advertisement. Council Policy 000-23 "Product Endorsement" and Administrative Regulation 95.65 "Product Endorsement" are incorporated by reference in this paragraph.

3.15 Duty to Disclose

Every employee shall immediately disclose the nature and extent of any interest, direct or indirect, which may conflict with his responsibility or duty, or which, because of his position, may influence a decision to the benefit of the organization in which he has an interest. Such disclosure shall be in the form of a memorandum to the City Manager, transmitted via the employee's department head.

3.16 Duty to Cooperate

Every employee shall cooperate fully with judicial bodies and courts, and with lawfully constituted investigative commissions, committees, bodies and juries; appear before them upon request; and answer all questions concerning his conduct in office or his performance of official duties or matters within his knowledge pertaining to the property, government or affairs of the City of San Diego. Failure to do so shall be cause for appropriate disciplinary action, including possible dismissal from City service.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|--------------------------------|------------|----------------|
| SUBJECT CONFLICT OF INTEREST AND EMPLOYEE CONDUCT | Number 95.60 | Issue 2 | Page 8 of 8 |
| | Effective Date May 23, 1990 | | |

APPENDIX

Legal References

California Government Code section 87100 et seq.

California Government Code section 1090 et seq.

Administrative Regulation 45.50 PRIVATE USE OF CITY EQUIPMENT AND MATERIALS
PROHIBITED

City Charter

Council Policy 000-4 CODE OF ETHICS

Municipal Code

Personnel Manual Section A-2 COMMISSION POLICY STATEMENT: MOTOR VEHICLE
VIOLATIONS

Personnel Manual Section G-1 CODE OF ETHICS AND CONDUCT

Personnel Manual Section G-6 REGULATION OF OUTSIDE EMPLOYMENT OR ENTERPRISE

Personnel Manual Section L-2 SEPARATION AND DISCIPLINARY ACTIONS: DISCIPLINE

Subject Index

Ethics

Conflict of Interest

Employee Conduct

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|---------------------------------|------------|----------------|
| SUBJECT EQUAL EMPLOYMENT OPPORTUNITY POLICY AND COMPLAINT RESOLUTION PROCEDURES | Number 96.50 | Issue 2 | Page 1 of 8 |
| | Effective Date June 22, 2018 | | |

1. PURPOSE

- 1.1. To reaffirm and communicate the City of San Diego's commitment to the principles of equal opportunity and to a work environment free of discrimination, harassment and retaliation.
- 1.2. To establish procedures for effectively handling *Reports* of potential violation of the City's Equal Employment Opportunity Policy when such *Reports* are brought forward within City departments, and to ensure that *Reported* issues are resolved in a prompt, appropriate and consistent manner which supports and promotes the well-being of employees as well as the business needs of the City.

(*Reports* of EEO Policy violations which are filed with the Personnel Department's *Equal Employment Investigations Office* will be handled pursuant to Civil Service Rule XVI and Personnel Manual Index Code K-2. See Section 5.8.1 for additional *Reporting* options available to employees).

2. SCOPE

- 2.1. This policy shall apply to all employees in the City of San Diego, including contract employees, interns and volunteers.

3. DEFINITIONS

- 3.1. *Equal Employment Opportunity Committee (City EEOC)* – Committee composed of representatives from the Human Resources Department, the City Attorney's Office, *Equal Employment Investigations Office*, and representative managers from operating departments, which meets on a periodic basis to review and recommend changes in the City's EEO policies and procedures.
- 3.2. *Equal Employment Investigations Office (EEIO)* – Located within the Personnel Department, this office is responsible for the administration of the City's internal program for the investigation and resolution of *Complaints* or charges of unlawful discrimination based upon Title VII of the Civil Rights Act of 1964. The *EEIO* acts as the City's liaison and primary contact with all Federal and State compliance agencies. As such, it is the duty of the *EEIO* to officially receive and process formal *Complaints* lodged by the agencies;

(Supersedes Administrative Regulation 96.50, Issued 1, effective September 5, 2000)

Authorized

Signature on File
CHIEF OPERATING OFFICER

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|---------------------------------|------------|----------------|
| SUBJECT EQUAL EMPLOYMENT OPPORTUNITY POLICY AND COMPLAINT RESOLUTION PROCEDURES | Number 96.50 | Issue 2 | Page 2 of 8 |
| | Effective Date June 22, 2018 | | |

investigate and respond to such *Complaints*; arrange and schedule employee interviews and provide access to relevant records when requested by the state or federal agent or officer; and to receive and respond to any findings of fact presented by the compliance agencies as a result of their investigation. In addition, the *EEIO* receives internal *Complaints* directly or indirectly from applicants for City employment, employees, former employees, contract employees, interns, and employee representatives.

- 3.3. Department Head – All *Department Directors* and *Executive Directors* responsible for a Department or a Program.
- 3.4. Deputy Director - For this A.R., “*Deputy Director*” shall mean all positions given the Appointing Authority responsibility generally exercised by the head of a division, or major sub unit, within a department.
- 3.5. Supervisor – Any employee who has authority to undertake or recommend employment decisions, including authority to direct the daily work activities, review work performance, and recommend or implement disciplinary actions affecting one or more City employees. This includes first-level *Supervisors* and above.
- 3.6. Complaint (or Report) – An allegation of potential violation of the City’s EEO Policy, as documented on an EEO *Report* Form (see EDP-100).
- 3.7. Complainant (or Reporting Employee) – An individual *Reporting* a potential violation of the City’s EEO Policy.
- 3.8. Subject Employee – An individual who has allegedly violated the City’s EEO Policy.

4. POLICY

- 4.1. The City of San Diego’s Equal Employment Opportunity Policy is incorporated into this Administrative Regulation by reference as if fully duplicated at this point.

5. RESPONSIBILITY

- 5.1. *Equal Employment Opportunity Committee (City EEOC)*

The *City EEOC* will serve as the City’s working body for the review of Citywide EEO policies and procedures. This committee will meet periodically to discuss changes in federal and state EEO law and their impact on City procedures and policies; will review unique or atypical EEO *Complaints* and investigations to ensure procedural issues are adequately addressed; will review the impact this Administrative Regulation has on improving the City’s EEO *Complaint* resolution efforts; and will educate and inform departments on EEO issues.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|---------------------------------|------------|----------------|
| SUBJECT EQUAL EMPLOYMENT OPPORTUNITY POLICY AND COMPLAINT RESOLUTION PROCEDURES | Number 96.50 | Issue 2 | Page 3 of 8 |
| | Effective Date June 22, 2018 | | |

5.2. Human Resources Department

The Human Resources Department will serve as an additional resource regarding individual or Citywide EEO policy issues.

5.3. Personnel Department - *Equal Employment Investigations Office (EEIO)*

It is the responsibility of the *EEIO* to record, track, and periodically review *Complaint* filings to identify potential areas of concern with regard to the timeliness of investigation and the resolution of complaints by departments. (Additional responsibilities of this office are outlined in Personnel Manual Index, Code K-2.)

5.4. City Attorney's Office

The City Attorney's Office shall review and disseminate, on an ongoing basis, any changes to the statutory requirements concerning EEO issues. The City Attorney's Office shall also review new cases interpreting the statutes. Any changes in the laws will be brought before the EEO Committee, which will review such changes and recommend necessary City-wide policy revisions.

5.5. *Deputy Director*

The *Deputy Director* shall be responsible for ensuring that individual *Reports* of potential EEO Policy violations are processed and resolved consistent with this regulation. The *Deputy Director* will be accountable for monitoring patterns of *Complaints* within their areas of responsibility and for ensuring that steps are taken to address potential violations on a preventive basis.

5.6. *Supervisors*

- 5.6.1. *Supervisors* are required to monitor City workplaces for actual or alleged violations of the EEO Policy and to take steps to stop actions contrary to these policies when they occur. Specifically, *Supervisors* shall:
- a. use appropriate education and training measures to both inform employees regarding the City's EEO Policy, and to ensure that employees are aware of the procedures for *Reporting* potential policy violations;
 - b. stop behavior in violation of the City's EEO Policy when directly observed or upon direct knowledge of;
 - c. ensure that instances of actual or potential EEO Policy violations are *Reported* as outlined in Section 5.8, below;

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|---------------------------------|------------|----------------|
| SUBJECT | Number 96.50 | Issue 2 | Page 4 of 8 |
| EQUAL EMPLOYMENT OPPORTUNITY POLICY AND COMPLAINT RESOLUTION PROCEDURES | Effective Date June 22, 2018 | | |

- d. manage the effect in the workplace of EEO Policy violation *Reports* by maintaining confidentially, insofar as practical, regarding the allegations, the *Complainant* and other identified individuals; and
- e. ensure that individuals involved in EEO investigations, either as the *Complainant*, *Subject Employee*, or as a witness, are not subjected to direct or indirect retaliation.

5.7. Employees

- 5.7.1. It is the City's policy that employees must set an example of acceptable conduct and will not participate in or provoke behavior that is discriminatory, harassing, or retaliatory.
- 5.7.2. Employees who observe or feel they have been subjected to conduct in violation of the City's EEO Policy should *Report* these as outlined in Section 5.8.1, below.
- 5.7.3. In addition, employees are responsible for maintaining confidentiality when they participate in a *Complaint* process as a witness, subject or *Complainant*.

5.8. *Report* Origination Procedure

- 5.8.1. If an employee believes that a violation of the City's EEO Policy has occurred, she/he is encouraged to *Report* these instances immediately to any of the following (the employee does not have to follow the departmental or divisional chain of command):
 - a. The employee's *Supervisor*;
 - b. Another *Supervisor* within or outside the employee's "chain-of-command"
 - c. The employee's *Deputy Director*, or *Department Head*
 - d. The departmental Human Resources office
 - e. The Human Resources Department (619) 236-6313
 - f. The Personnel Department's EEIO, at:
1200 3rd Avenue, Suite 1501
San Diego, CA 92101
Telephone: (619) 236-7133
Fax: (619) 236-7138
The time frame for filing a *Complaint* is one year from the most recent incident.
 - g. The State of California Department of Fair Employment and Housing (DFEH), at:
Telephone: (800) 884-1684
Website: <http://www.dfeh.ca.gov>
The time frame for filing DFEH *Complaints* is one year from the date of the alleged violation.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|---------------------------------|------------|----------------|
| SUBJECT EQUAL EMPLOYMENT OPPORTUNITY POLICY AND COMPLAINT RESOLUTION PROCEDURES | Number 96.50 | Issue 2 | Page 5 of 8 |
| | Effective Date June 22, 2018 | | |

- h. U.S. Equal Employment Opportunity Commission (U.S. EEOC), at:
555 West Beech Street, Suite 504
San Diego, CA 92101
Telephone: (619) 557-7235
Website: www.eeoc.gov
The time frame for filing U.S. EEOC *Complaints* is 180 days from the date of the alleged violation.

- 5.8.2. If the employee *Reports* possible violations to any of the above, the *Complaint* procedures listed in this section shall apply.
- a. *Complaints* filed with the Personnel Department's *EEIO* will be subject to procedures detailed in Personnel Manual Index Code K-2.
 - b. *Complaints* filed with the DFEH or U.S. EEOC will be subject to procedures of the respective agencies.
 - c. The ability to complete an effective and thorough investigation is in part dependent upon the length of time between the alleged act and when it is *Reported*.

5.9. *Complaint Intake Procedure*

- 5.9.1. *Supervisors* shall complete and forward to their *Deputy Director*, an Equal Employment Opportunity *Report* Form in any of the following instances:
- a. an employee expresses a desire to file a *Complaint* of potential EEO Policy violation;
 - b. discussions with an employee leads the *Supervisor* to believe that an EEO Policy violation with regard to workplace harassment may have occurred, whether or not the employee wishes a *Complaint* filed; or
 - c. a *Supervisor* determines that observed employee behavior is one which is contrary to City's EEO Policy and which will likely lead to written discipline.
- 5.9.2. Instructions on proper EEO *Report* Form completion and routing, including key information to be aware of when taking an employee *report*, are found on the back of the form.
- 5.9.3. When completing the EEO *Report* Form, the *Supervisor* shall:
- a. also inform the *Complainant* of the alternate *Reporting* avenues listed in Section 5.8.1;
 - b. advise the employee that confidentiality will be maintained to the highest degree possible, but cannot be guaranteed; advise the employee of his/her responsibility to protect confidentiality;
 - c. inform the employee that she/he will be officially notified of *Complaint* results; and

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|--|---------------------------------|------------|----------------|
| SUBJECT | Number 96.50 | Issue 2 | Page 6 of 8 |
| EQUAL EMPLOYMENT OPPORTUNITY POLICY AND COMPLAINT RESOLUTION PROCEDURES | Effective Date June 22, 2018 | | |

- d. emphasize that if the employee feels she/he is being retaliated against, she/he should notify any of the individuals listed in Section 5.8.1 above immediately.

These points are summarized on the Employee Record portion of the EEO *Report* Form, (see EDP 100) which the *Supervisor* and *Employee* shall sign for the record.

- 5.9.4. All *Complaints* received shall be held in strict confidence to protect individual privacy rights and the reputations of those involved, and will be shared only with individuals who have a legitimate operational responsibility for investigating or resolving the issues identified.

5.10. EEO *Report* Form Review and Delegation for Action

- 5.10.1. The *Deputy Director* shall review the EEO *Report* Form and determine what, if any, additional action will be taken (e.g. formal fact finding) including by whom and when. The *Deputy Director* shall route a preliminary copy of the EEO *Report* Form to the *EEIO* through confidential transmittal, and refer, if appropriate, the *Reported* issue(s) to the delegated staff member for follow-up action, to be completed within 60 days absent extenuating circumstances.
- 5.10.2. A management designee, shall review the final results of any investigatory or follow-up action for thoroughness and consistency with established EEO policies, procedures and City-wide investigatory practices. (For actions involving formal fact finding investigations, refer to the Dimensions in Discipline training manual, which outlines appropriate procedures for effectively completing these types of investigations.)
- 5.10.3. Upon the conclusion of the follow-up action, notification is made to the *Reporting* and *Subject Employees* that the preliminary investigation, or follow-up action, has been completed. (No *Report* Determination information, such as that outlined in Section 5.11.1, is shared at this time.) The *Subject* and *Reporting Employee* are also notified that they will be informed of final determination subsequent to any disciplinary action and appeal, within an additional 60 days.

5.11. *Report* Determination and Close-Out

- 5.11.1. Upon conclusion of the disciplinary process and appeal, if any, the *Deputy Director* shall record the final determination of the *Complaint* on the EEO *Report* Form, based on the following classifications:
 - a. Unfounded – The alleged act(s) did not occur.
 - b. Not Sustained – Follow-up investigation could not clearly prove or disprove the allegations

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|---------------------------------|------------|----------------|
| SUBJECT EQUAL EMPLOYMENT OPPORTUNITY POLICY AND COMPLAINT RESOLUTION PROCEDURES | Number 96.50 | Issue 2 | Page 7 of 8 |
| | Effective Date June 22, 2018 | | |

- c. No Violation – Alleged act(s) did not violate any City Policy
- d. Violation of City EEO Policy – Alleged act(s) occurred and violate the City’s EEO Policy.
- e. Violation of City Policies – Alleged act(s) occurred and violate City Policy(ies).

5.11.2. The *Deputy Director* or his/her designee will ensure that the *Reporting* and *Subject Employees* are notified of the final determination of the *Complaint*, based on the classifications above. The date of notification and the signature of the individual performing the notification shall be recorded on the *EEO Report Form*.

5.11.3. The *Deputy Director* shall ensure that appropriate disciplinary measures are taken against any employee who violates the City’s EEO Policy or procedures. The final action(s) resulting from the *Complaint* (e.g., reprimand, counseling) is recorded on the *Complaint* form.

5.11.4. The *Deputy Director* shall designate appropriate follow-up contact with the *Complainant*, witness, or others who may have participated in any investigation, to ensure that direct or indirect retaliation has not taken place. Follow-up action(s) to be performed are recorded on the *EEO Report Form* in the space provided. The original form is then signed by the *Deputy Director* and forwarded to the *EEIO* for records retention.

5.12. Records Maintenance

5.12.1. The Personnel Department’s *EEIO* shall maintain a record of *Report Form* filings. The *EEIO* shall maintain these records in such a fashion that a list of *EEO Report* filings whose final determinations have not been completed within 120 days shall be forwarded to the respective *Department Heads* to ensure prompt completion, absent extenuating circumstances. This 120 day period is defined as the time between the date of *Report* filing and notification to the *Reporting Employee* of the final *Complaint* determination.

5.12.2. The *EEIO* will review incoming *EEO Report Form* filings and bring forward to departments any specific issues regarding these filings, based upon the circumstances surrounding individual policy violations or violation trends.

5.12.3. The *EEIO* will maintain the confidentiality of *EEO Report Form* records by releasing information only at the request of *Department Heads*, *Deputy Directors*, or appropriate designees for good and sufficient cause.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| | | | |
|---|------------------------------------|------------|----------------|
| SUBJECT EQUAL EMPLOYMENT OPPORTUNITY POLICY AND COMPLAINT RESOLUTION PROCEDURES | Number 96.50 | Issue 2 | Page 8 of 8 |
| | Effective Date November 8, 2017 | | |

APPENDIX

Legal References

Civil Service Rule XVI - Discrimination *Complaints*
Personnel Manual Index Code K-2, Discrimination *Complaint* Procedures
“Fact Finding Investigations” - Dimension in Discipline Manual
Equal Employment Opportunity Policy – Annual Statement

Forms

Equal Employment Opportunity *Report* Form (EDP-100)

Subject Index

Personnel
Equal Employment Opportunity Policy and *Complaint* Resolution Procedures

Administering Department

Personnel Department



THE CITY OF SAN DIEGO
**Equal Employment Opportunity
REPORT FORM (AR 96.50)**

(SEE REVERSE OF PAGE 3 FOR INSTRUCTIONS)

Ref- _____

1 NAME (TYPE OR PRINT) _____ SS# _____ DATE _____

JOB CLASS _____ DEPT./DIV. _____

WORK LOCATION _____ SUPERVISOR _____

WORK PH. _____ (ALTERNATE PH. _____) WORK PH. _____

2 CONCERNS EXPRESSED BY EMPLOYEE (WHO, WHAT, WHERE, WHEN, HOW LONG HAS THIS BEEN GOING ON? HAVE YOU TOLD ANYONE ELSE?):

☐ WITNESS LIST ATTACHED
☐ ADDITIONAL PAGES ATTACHED

3 WHY DOES THE EMPLOYEE FEEL THE ABOVE EVENT(S) IS / ARE OCCURRING?

☐ ADDITIONAL PAGES ATTACHED

REMEDY SOUGHT BY EMPLOYEE:

☐ NO REMEDY SOUGHT

4 IMMEDIATE CORRECTIVE ACTION TAKEN, IF ANY (NON-DISCIPLINARY):

☐ ADDITIONAL PAGES ATTACHED

5 FILING AND ROUTING RECORD:
REPORTING SUPERVISOR: _____ SIGNATURE _____ DATE _____
ROUTED TO (PRINT): _____ SIGNATURE _____ DATE _____

6 EEO RELATED: ☐ RACE/ETHNICITY/NATIONAL ORIGIN ☐ GENDER ☐ RELIGION ☐ SEXUAL ORIENTATION ☐ AGE
☐ DISABILITY/MEDICAL CONDITION ☐ MARITAL STATUS ☐ PREGNANCY ☐ SEXUAL HARASSMENT ☐ OTHER

☐ RETALIATION BASED UPON PREVIOUS COMPLAINT REGARDING:

☐ ACTION REQUIRED. REFERRAL TO:
☐ NO FURTHER ACTION REQUIRED (GO TO #8 BELOW)

FACT FINDING TO BE CONDUCTED BY:
TARGET COMPLETION DATE:

COMMENTS:

☐ ADDITIONAL PAGES ATTACHED

DEPUTY DIRECTOR (PRINT): _____ SIGNATURE _____ DATE _____
CC: PERSONNEL DEPARTMENT - EQUAL EMPLOYMENT INVESTIGATIONS OFFICE

7 PRELIMINARY NOTIFICATION TO

REPORTING EMPLOYEE: BY _____ DATE _____

SUBJECT: BY _____ DATE _____

8 REPORT DETERMINATION: ☐ UNFOUNDED ☐ NO VIOLATION ☐ VIOLATION OF CITY / DEPT. EEO POLICY(IES)
☐ NOT SUSTAINED ☐ VIOLATION OF OTHER CITY / DEPT. POLICY(IES)

FINAL NOTIFICATION TO:
☐ EMPLOYEE BY _____ DATE _____ ☐ SUBJECT BY _____ DATE _____

9 FINAL ACTION(S) RESULTING FROM EEO REPORT:

☐ NO ACTION(S) REQUIRED ☐ RESULTING DISCIPLINE BASED SOLELY ON NON-EEO POLICY VIOLATIONS

10 SPECIFY FOLLOW-UP MONITORING TO BE PERFORMED BY: _____ DATE: _____
COMMENTS:

DEPUTY DIRECTOR (PRINT): _____ SIGNATURE _____ DATE _____

ROUTE TO: PERSONNEL DEPARTMENT - EQUAL EMPLOYMENT INVESTIGATIONS OFFICE

REF: _____



THE CITY OF SAN DIEGO
Equal Employment Opportunity

REPORT FORM RECEIPT

Ref- _____

REPORTING SUPERVISOR RECORD

ROUTED TO (PRINT) _____ SIGNATURE _____ DATE _____

ROUTED TO (PRINT) _____ SIGNATURE _____ DATE _____

This portion of the Report Form Receipt is retained by the Reporting Supervisor as a record of timely forwarding. **Do not keep any copies of the original Report Form.**

As a supervisor, you are responsible for managing the effect reports of potential EEO policy violations have in the workplace by maximizing confidentiality, insofar as practical, regarding the allegations, the reporting Employee, and other identified individuals. The information relayed to you in this Report is confidential and should not be shared with others unless there is a specific need to know.

In addition, your responsibilities include ensuring that individuals involved in EEO investigations, either as a reporting Employee or as a witness, are not subjected to direct or indirect retaliation.

Refer to AR 96.50 regarding the City's procedure for handling reports of potential EEO policy violations.

(TEAR GOLDENROD COPY ALONG DOTTED LINE)

EMPLOYEE RECORD

Thank you for coming forward with your concern regarding potential violation(s) of the City's Equal Employment Opportunity Policy. This notification copy is being provided to you as a record of your report and as assurance that prompt and appropriate action will be taken on the issues you raised. The City would like to officially advise you of the following:

1. You have the right to report any conduct which you believe violates the City's Equal Employment Opportunity Policy. Your report is taken seriously and will be investigated pursuant to EEO procedures detailed in AR 96.50.
2. In addition to filing this report with your Department, you also have the right to file a complaint directly with any of the following agencies: the City's Labor Relations Office (619)236-6313; the City's Employee Development Program (619) 235-5802; the City's Equal Employment Investigations Office (619) 236-7133; the State of California Department of Fair Employment and Housing (800) 884-1684; or the US Equal Employment Opportunity Commission (619) 557-7235. You should contact these agencies directly to determine the time frames for complaint filing.
3. The information you reported will be confidential to as great a degree as legally permissible and reasonably practical. While your expressed desire regarding confidentiality will be seriously considered, those wishes must be weighed against: 1) the responsibility of the City to investigate possible EEO violations and to take corrective and preventive action where appropriate, and; 2) the right of the accused employee to obtain information about the allegation. During any investigation, the subject employee has a right to the name of the reporting Employee and the information related to alleged acts, but the names of witnesses will not be disclosed. In all cases, your report will only be discussed with those who have a legitimate responsibility for investigating or resolving the issues identified.
4. You have a responsibility to protect the confidentiality of this report by not discussing these issues in the workplace. Questions regarding what follow-up action has or will occur should be directed to one of the following individuals: the person with whom you filed this report, your Deputy Director, Department Director, or the City's Equal Employment Investigations Office. By doing so, you help to minimize workplace disruptions, preserve the reputations of all parties involved, and help to preserve the integrity of any investigation which may follow.
5. You will be notified of the final results of this report. Should you not receive such results within 120 days, you should follow up with your Deputy Director, Department Director, or the City's Equal Employment Investigations Office by referring to the EEO Report Form Reference number below. Information regarding what, if any, disciplinary action has been or will be taken against other individuals will not be disclosed.
6. Retaliation towards you for filing this report is illegal and will not be tolerated. If you feel that you are being retaliated against, please contact your Deputy Director, Director, Human Resource Manager, or EEO unit; or any of the contacts listed in 2, above.

EMPLOYEE _____ SIGNATURE _____ DATE _____

REPORTING SUPERVISOR _____ SIGNATURE _____ DATE _____

REF: _____

(Reference A.R. 96.50)

The EEO Report Form and Report Form Receipt are used to record and track a report of alleged violations of the City's Equal Employment Opportunity Policy. Supervisors are required to use this form whenever allegations of EEO policy violations are brought to their attention. This generally occurs in three ways: 1) an employee expresses a desire to formally file a report of EEO violation; 2) a supervisor observes employee behavior contrary to City's EEO policy which may warrant written discipline; and 3) discussion with an employee leads the supervisor to believe that an EEO policy violation regarding workplace harassment may have occurred, **whether or not the employee wishes a complaint filed**. While it may seem reasonable to let the employee determine whether to pursue a complaint, the City must fulfill its responsibility to prevent discrimination and harassment and to take corrective action despite the employee's wishes.

INSTRUCTIONS:

(For these instructions, "Deputy Director" is an individual who is given the Appointing Authority responsibility generally exercised by the head of a division, or major sub-unit, within a department; "Employee" is the person reporting the potential violation; "Reporting Supervisor" is the supervisor or EEOL to whom the report is made; and "Subject" is the individual who has allegedly violated the EEO Policy.)

① The Employee or Reporting Supervisor completes the top portion of the form which records general information on the Employee. Social Security Number is requested because the City uses this number as the Employee Identification Number to track employees throughout its personnel systems.

② The Reporting Supervisor completes this section by recording the alleged policy violations as relayed by the Employee (or as directly observed). Key elements to record are listed (*who, what, where, when*). In addition, it is important to record how long the alleged violations may have been occurring. For example, "*at least two weeks*"; "*since John was promoted*". Ask about and record the names of any individual who may be a potential witness to the allegations. Ask if the Employee has spoken to anyone about this or has spoken with the person who allegedly violated the policy. Ask about any written documentation which may support the allegations. If the Employee has these, attach them to the form, but instruct the Employee not to go "hunting for evidence" if s/he does not already have documentation.

③ Record here the reason the Employee feels the reported actions have occurred. Examples may include: favoritism, conflict of interest, poor supervision, discrimination, lack of knowledge. "Remedy Sought" may include reassignment, correction of problem, or simply "wanted to inform supervisor."

④ The Reporting Supervisor records what, if any, immediate action was taken in response to the reported act. In all instances it is critical that no formal discipline, such as counselings or reprimands, be taken until directed to do so.

The Reporting Supervisor and the Employee both sign the bottom of the Report Form Receipt (EDP 100A). A copy of the bottom half is retained by the Employee as his/her record of report filing.

⑤ The Reporting Supervisor routes the form to his/her Deputy Director, obtaining the signature of the Deputy in the spaces provided on the Report Form and top half of the Report Form Receipt. Use routing methods consistent with those used for other highly confidential material. The Reporting Supervisor retains a copy of the top half of the Report Form Receipt as record of routing.

⑥ The Deputy Director reviews the information and records what follow-up action, if any, will be performed within 60 days. The Deputy also makes a preliminary assessment regarding the specific EEO "protected status" (e.g. race, religion, gender, etc.) to which the complaint may be related. In the event of unique or serious circumstances, contact is made with Personnel Department's Equal Employment Investigative Office (619) 236-7133 to ensure a suitable course of action.

A copy of the Report Form is sent via confidential transmittal to the Personnel Department's Equal Employment Investigative Manager to initiate proper tracking of the EEO Report Form.

⑦ Upon completion of follow-up action, such as a fact finding investigation, preliminary notification is made to both the Employee and Subject that follow-up action has been completed and additional action, including discipline and related appeal, if any, will be completed within 60 days. Record this preliminary notification including the name of the person performing the notification and the date.

⑧ Upon conclusion of the disciplinary process, final determination is recorded by checking the relevant box(es):

Unfounded: The alleged acts did not occur.

Not Sustained: Follow-up investigation could not clearly prove or disprove the allegations.

No Violation: Alleged acts did not violate any City policy(ies).

Violation of City / Dept EEO policy(ies): Alleged act(s) occurred, and some or all violate City / Dept EEO policy(ies).

Violation of Other City policy(ies): Alleged act(s) occurred, and some or all violate non-EEO policy(ies).

The Deputy Director then ensures that the Employee and the Subject receive notification of this information. **Disciplinary action, if any, is not shared.** Record notification information in the space provided.

⑨ Any action, such as discipline, which results from the EEO report is recorded here.

⑩ Key to demonstrating the City's commitment to a long-term EEO discrimination prevention program is regular follow-up, typically 3 and 6 months after the final resolution, with the Employee and witnesses to ensure that retaliatory actions have not occurred. In the space provided, indicate the nature and date of follow-up action(s) to be performed. For example, include the names of those to be contacted, the date and the name of individual delegated to follow-up.

**Commission on Police Practices
Training Academy**

August 29, 2023

5:30pm - 7:30pm

Component 1 (Completed)

Introducing New Commission to Oversight of Law Enforcement, Brown Act, Case Review Process

- Brief History of CPP & Creation of OCPP
- Highlights of Ralph M. Brown Act
- Overview of Interim CPP Case Review Process

Location

Procopio Tower

Conference Room, First Floor

525 B St – San Diego, CA 92101

September 12, 2023

4:30pm – 7:30pm

Component 2 (Completed)

Operational Procedures, Case Review, & Deciding on Dates for Future Meetings

- Governance Operational Items -CPP Officers, Temporary Bylaws
- Reimaging CPP Case Review & Backlog of Cases
- Future Dates CPP Regular Business Meetings

Location

Valencia Park/Malcolm X Branch Library

5148 Market Street – San Diego, CA 92114

September 19, 2023

9:30am-12pm

Component 3 Cohort 1 (Completed)

Understanding the functions of various departments within SDPD Headquarters (Communications/Sally Port/Forensics)

- SDPD Headquarters Tour
- Name Badges & Parking Placard for Commissioners
- Meeting with SDPD Leadership & IA Staff

Location

San Diego Police Headquarters, Room 213

1401 Broadway – San Diego, CA

**Commission on Police Practices
Training Academy**

September 19, 2023

4:30pm-7:30pm

Component 4 (Completed)

Training Schedule, Brown Act, Administrative Regulations

- Recommended CPP Training Schedule
- Overview of the Ralph M. Brown Act (Part1)
- Confidentiality Requirement

Location

Skyline Hills Branch Library

7900 Paradise Valley Road – San Diego, CA

September 23, 2023

8:30am - 3:00pm

Component 5 (Cohort 1 - 7 Commissioners) (Completed)

SDPD Use of Force, Detention, Laws of Arrest Procedures, Simulators

Location

Police Plaza

4020 Murphy Canyon Rd – San Diego, CA

October 7, 2023

11am – 3:30pm

Component 6 (Completed)

Focusing on Brown Act, Steps in Case Review, 4th Amendment & Search and Seizure

- Overview of the Ralph M. Brown Act (Part2)
- How to Review a Case
- 4th Amendment, Waiver & Search and Seizure
- Deliberation of Cases

Location

Logan Heights Branch Library

567 South 28th Street – San Diego, CA

October 14, 2023

10:30am – 3:30pm

Component 7

Presentation by ACLU, Distribution of Laptops to Commissions with Instructions on Usage, City Administrative Regulations & Case Deliberation

- Deliberation of Cases
- Racial Profiling & Law Enforcement in San Diego (ACLU San Diego)

Commission on Police Practices Training Academy

- Distribution of Laptops & Instructions for Usage
- City Administrative Regulations

Location

**Mira Mesa Branch Library
8405 New Salem Street– San Diego, CA**

October 21, 2023

8:00am – 1:00pm

Component 8 (Cohort 2-10 Commissione)

Commissioners who have not already taken this training should sign up with staff asap.
SDPD Use of Force, Detention, Laws of Arrest Procedures, Simulators

Location

**Police Plaza
4020 Murphy Canyon Rd – San Diego, CA**

October 24, 2023

9:30am-12pm

Component 9 (Cohort 2-10 Commissioners)

Commissioners who have not already taken this training should sign up with staff asap.

Understanding the functions of various departments within SDPD Headquarters (Communications/Sally Port/Forensics)

- SDPD Headquarters Tour
- Name Badges & Parking Placard for Commissioners
- Meeting with SDPD Leadership & IA Staff

Location

**San Diego Police Headquarters, Room 213
1401 Broadway – San Diego, CA**

October 24, 2023

4:30pm-7:30pm

Component 10

Legal Perspective on topics covered by SDPD & Deliberation of Cases Approaching 1 year

- Legal Perspective of SDPD Officers Use of Force (including deadly force), Arrest and Detention, Search & Seizure

Presenter: CPP Outside Counsel Duane Bennett

**Commission on Police Practices
Training Academy**

- Deliberation of Cases

Location

Skyline Hills Branch Library

7900 Paradise Valley Road – San Diego, CA

November 7, 2023

4:30pm-7:30pm

Component 11

Regular Business Meeting & Training

- Presentation on the Parliamentary Procedure
- CPP Policies & Procedures – Bylaws, Standard Operating Procedures, Implementation Ordinance

Location

Skyline Hills Branch Library

7900 Paradise Valley Road – San Diego, CA

November 28, 2023

4:30pm – 7:30pm

Component 12

Administrative Operations, Overview of Peace Officer Bill of Rights & NACOLE Best Practices

- Better Management Impact System – Tracking Commissioner Hours
- Overview of POBOR (CPP Outside Counsel Duane Bennett)
- Shared Information Learned from NACOLE Annual Conference (CPP Cabinet)

Location

Valencia Park/Malcolm X Branch Library

5148 Market Street – San Diego, CA 92114

November 2023

3:30 – 7:30pm

Component 13

SDPD Policies & Procedures Training, Internal Affairs Complaint Process, Ride-Alongs (*IA Captain*)

Location

San Diego Police Headquarters

1401 Broadway – San Diego, CA

**Commission on Police Practices
Training Academy**

November 2023

Component 13

Panel Presentations on Civil or Human Rights,
Criminal Justice, Youth, Mental Health,
Impacted Individuals

Community Perspective & Experiences and
Training Required by the Implementation
Ordinance

Rebuilding Community-Government
Relationships (Tasha Williamson)

Diversity, Sensitivity & Implicit Bias Training

Location: TBD