IT Policy and Project Updates

REDONDO BEACH

Mike Cook – IT Director
March 3, 2026

Video Policy Updates

New process for approvals

Criteria for new sites

Aligns policy with management best practices

Updated site listing

Clear documentation of access, storage and retention

Artificial Intelligence Policy

artificial intelligence (AI), the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings… systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.

Artificial Intelligence Policy

Establishes rules and approval processes for the usage of AI tools

Encourages experimentation while preserving cybersecurity standards and compliance

Prevents unauthorized use of AI technologies particularly those involving sensitive data

Alignment with Projects and Strategy

AI Policy will feed in to City-Wide AI Strategy

- Likely discussion topic at upcoming Strategic Planning Session
- Generative AI, Web Bots, Building/Planning, Procurement
- AI will increasingly be integrated into existing platforms

Surveillance Camera Stabilization and Site Review

Citywide Digitization and Electronic Workflows

Both AI and Cameras likely to be included in Budget process for FY26-27

Alignment with Projects and Strategy

City-Wide Digitization and Workflow
HR Digital Onboarding
Enterprise Knowledge Capture and Training
Generative AI Product Selection
Department-Specific AI Strategy
Grant Identification and Application
Privileged Access Modernization (Police)
Credential Consolidation Initiative for PD
Public Records Request System
Rubrik M365 Backup Extension
Work Management Platform Selection

Business Licensing System Modernization
Finance Workflows and Self Service
HR Systems Improvements
Remote-Site Network Improvements
Broadcast Services for Performing Arts Center
Seaside Lagoon Improvements
Enterprise Asset Management
Cybersecurity Self-Assessments
Network Segmentation & Hardening
Measure FP Implementation
Council Chambers HD and Broadcast Upgrades

Other Updates

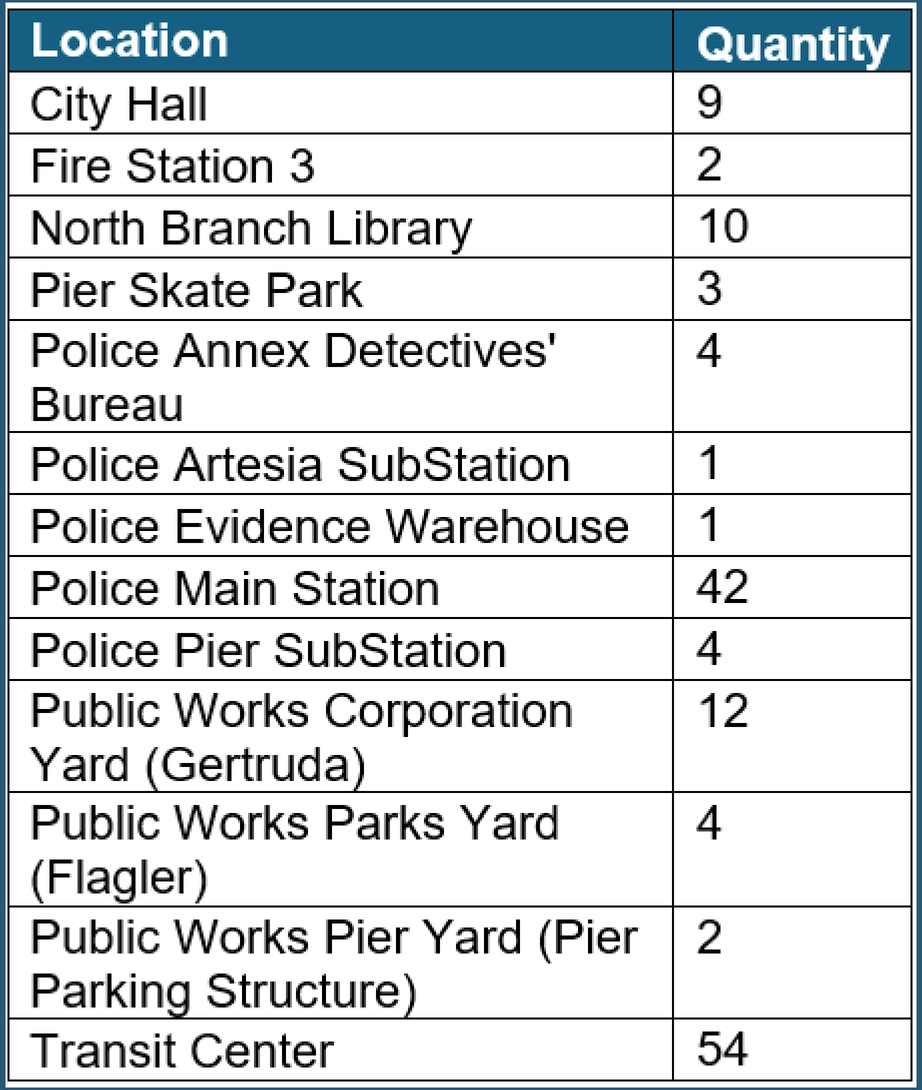
4.01 Responsible Use – Updates 2008 policy modernizes approach to privacy and policy. Limits use of unauthorized tools for city business. Expands on cybersecurity controls.

4.03 Email Communication – Minor updates. Discourages use of city email for personal business. Formalizes timing for disabling accounts. Expands scope of policy to include Redondo.gov.

4.02 E-Gov Steering Committee – Formally retires 2002 policy in favor of more collaborative and modern technology proposal processes

Discussion & Recommendation

- Recommendation to receive and file APP 10.57 Video Security, APP 10.57 Exhibit A Sites, and APP 4.05 Artificial Intelligence



Location	Quantity
City Hall	9
Fire Station 3	2
North Branch Library	10
Pier Skate Park	3
Police Annex Detectives' Bureau	4
Police Artesia SubStation	1
Police Evidence Warehouse	1
Police Main Station	42
Police Pier SubStation	4
Public Works Corporation Yard (Gertruda)	12
Public Works Parks Yard (Flagler)	4
Public Works Pier Yard (Pier Parking Structure)	2
Transit Center	54

CITY OF REDONDO BEACH		ADMINISTRATIVE POLICY AND PROCEDURES (APP)
Number: 04-01		**Subject:** Information Technology Responsible Use Policy
Original Issue: 08-18-95	**Effective:** 3/16/2026	**Category:** Information Technology
Supersedes: 07-01-08		

I. PURPOSE AND SCOPE

To establish guidelines for the responsible use of information technology (IT) resources throughout the City of Redondo Beach ("City").

City IT resources include, but are not limited to:

- Computing devices and related tools – desktops, laptops, tablets, smartphones, servers, printers, scanners, copiers, Internet access, wireless access, removable media (USB drives, etc.), e-mail (APP 4.03), cloud services licensed or authorized for use by the City, and the software that makes each tool functional.

- Communications tools – telephones, cellular phones (APP 2.09), voicemail, collaboration platforms (e.g., Microsoft Teams, Zoom), and other communication systems.

This policy applies to all City employees, contractors, volunteers, and other authorized users of City IT resources, whether accessing them on-site, remotely, or via cloud-based services. This policy does not apply to members of the public using public networks (i.e. Lagoon, Library, Visitor Wi-Fi).

II. GENERAL INFORMATION

A. City IT resources are made available to employees to improve efficiency, productivity, and communication.

B. All City IT resources are the property of the City and remain subject to City control. They are business tools and must not be abused.

C. City IT resources are to be used primarily for official City business. Limited incidental personal use is permitted, provided it does not:

- Interfere with job performance,
- Violate law or policy, or
- Pose a security or financial risk to the City.

D. Employees must comply with all applicable laws and regulations, including but not limited to the California Public Records Act, California Consumer Privacy Act, California Senate Bill 1386, HIPAA, CJIS, PCI-DSS and federal data protection requirements.

III. COMPUTING PRIVACY

A. All software, data, reports, email, voicemail, records, and information created, received, or stored on City IT resources (including cloud-hosted systems) are the property of the City. Authorized City staff may access them as necessary for business, legal, or security purposes. Access to a file or other electronic information does not imply permission to alter or destroy it.

B. There is no expectation of personal privacy when using City IT resources (including Wi-Fi). All use may be logged, monitored, or disclosed as required by law. City IT resources may be subject to remote access and/or administration by the Information Technology Department.

C. Users must not access another users account, copy, modify, or destroy another person's data without authorization.

D. Password sharing is prohibited. All users must use unique credentials and comply with City multi-factor authentication (MFA) and password requirements.

E. Confidential and personally identifiable information (PII) must be stored, transmitted, and accessed only in compliance with City data governance and retention policies.

VI. USAGE

A. IT resources must not be used to transmit, store, or access material that is obscene, derogatory, discriminatory, or otherwise conflicts with City personnel policies.

B. Employees share responsibility for protecting City IT resources against damage, misuse, or unauthorized access.

C. Personal use of City IT resources must be minimal and must not incur costs to the City. There is no expectation of personal privacy in the use of City IT resources. Computer files, no matter what medium they are stored or transmitted on may be subject to the California Public Records Act and may be subject to disclosure. IT equipment shall not be used for any commercial purpose.

D. Only IT staff may install, configure, or approve hardware, software, applications, browser extensions, or cloud integrations. Employee-owned devices may not be connected to the City wired network or protected City WiFi Networks (RBD, RBDOMAIN, RBMOBILE, SAFETY) unless explicitly authorized by the Information Technology Director. Personally owned devices may connect to the City's public networks (RBVISITOR, LAGOON, RBPL, RBSTAFF, RBPAC, RBTRANSIT, Pier Wifi, Pallet Shelter Wifi).

E. Files must be stored on City-approved network drives or cloud storage systems to ensure proper backup and retention. City workstations and laptops are not backed up individually; employees are encouraged to use approved storage. City data should primarily be stored in

City-approved systems (e.g., Microsoft 365). **Use of unauthorized cloud services for City business is prohibited.**

F. Employees must not input confidential, sensitive, or City-owned data into generative AI or automated tools without IT approval. AI tools may only be used in compliance with City security and privacy standards and all other APP's including APP4.05 Artificial Intelligence Policy.

G. Employees must never attempt to log in with another person's login, log in using administrative credentials without authorization, or share their own login credentials.

H. Workstations must be locked when unattended and logged off at the end of the day.

I. Sensitive data requiring encryption must be managed through City-approved tools. Decryption keys and passwords must be available to IT or Department Directors upon request.

J. Only IT staff may relocate, repair, or reconfigure City technology or communications equipment.

K. Only IT staff shall procure personal computers, tablets, cell phones, smart phones or servers. Purchases of computer equipment as part of other purchases (i.e. Building systems which provide servers, vehicle purchases which provide tablets, etc.) shall be approved by the Information Technology Director and the devices added to the City's technology management platforms and inventory. No departments shall operate information technology systems outside of the technological and cybersecurity controls implemented by the IT department.

L. Non-City personnel may only use City IT equipment with prior approval from the IT Director and relevant Department Head.

M. Remote Work Requirements – Employees working remotely must abide by the City's Remote Access Policy.

N. User accounts shall be disabled for any employee on work-leave (medical, administrative, etc.) and shall be disabled immediately upon separation.

V. CYBERSECURITY

A. The City uses modern endpoint detection and response (EDR) software, firewalls, and anti-malware systems to protect IT resources.

B. Employees must:
- Leave security software enabled at all times,
- Avoid opening suspicious emails or links, and
- Immediately report suspected security incidents, phishing attempts, or lost/stolen devices to IT and maintain confidentiality of reported cybersecurity events. Cybersecurity

incidents shall only be discussed on a need-to-know basis and official communications sent from the City Manager or his/her designee. Information pertaining to active cybersecurity threats, investigations or incidents shall not be discussed amongst coworkers who do not have a business need to know.

C. No one shall knowingly or maliciously introduce malware, hacking tools, or destructive code into City systems.

D. No one shall attempt to disable or circumvent city cybersecurity controls, including but not limited to firewalls, EDR software, identity management systems, physical security controls, hardware resets of devices, reinstallation of operating systems, etc.

E. No one shall attempt to guess, recover, change or otherwise access system administrator accounts without explicit written authorization from the Information Technology Department.

F. No City business shall be executed using an unauthorized VPN tool.

VI. PURCHASING

A. All technology hardware, software, cloud services, and upgrades must be reviewed and approved by IT prior to purchase to ensure compatibility, licensing compliance, and security.

B. All procurement must follow City purchasing procedures.

C. Equipment refresh and secure disposal of devices must be coordinated through IT.

D. All IT Equipment in excess of $800 initial purchase price must be tagged and tracked in the Information Technology Department inventory.

VII. INTERNET ACCESS

A. Internet access is provided to employees as a business tool.

B. All Internet activity is subject to monitoring, blocking and logging. Employees have no expectation of privacy when using City networks.

C. Prohibited uses include: Downloading non-business-related music, movies, obscene content, or software,
- Downloading copyright protected software or content without license,
- Accessing prohibited content including but not limited to, terrorism, crypto mining, . pornography, gambling, dating, weapons, etc.
- Circumventing security filters,
- Unauthorized use of social media or file-sharing services,
- Entering confidential data into unapproved AI tools or websites.

Authorization is granted for the purpose of legitimate investigative purposes

D. Limited streaming (training, webinars, City events) is permitted.

E. Displaying, storing, or transmitting offensive or sexually explicit content is strictly prohibited except where necessary by for legitimate investigative purposes.

VIII. EMAIL

Email is governed by APP 4.03 and subject to this policy. Employees must:
- Use City email accounts for all City business (not private accounts),
- Encrypt sensitive or confidential email as directed by IT,
- Report phishing attempts immediately,
- Comply with retention schedules.

IX. VIOLATIONS

Violations of this policy may result in:
- Restriction or revocation of IT access,
- Disciplinary action up to and including termination,
- Civil or criminal penalties for unlawful activity.

X. EXCEPTIONS

There will be no exceptions to this policy unless approved by the City Manager.

XI. AUTHORITY

By Authority of the City Manager

____
Mike Witzanksy

XII. ATTACHMENTS

N/A

CITY OF REDONDO BEACH		**ADMINISTRATIVE POLICY AND PROCEDURES (APP)**
Number: 04.03		**Subject: E-MAIL COMMUNICATION POLICY**
Original Issue: 04-01-03	**Effective:** 3/16/2026	**Category: INFORMATION TECHNOLOGY**
Supersedes: 04-01-03		

I. PURPOSE AND SCOPE

To define the proper use of the City of Redondo Beach e-mail processing system. These procedures apply to employees, advisory body members, council members, contractors, volunteers, and all others when they are using the City-provided e-mail processing system.

II. GENERAL INFORMATION

The City provides the following forms of electronic communications, messaging agents and electronic facilities: internal and external electronic mail (e-mail), telephone voice mail, Internet access, photocopy machines, facsimile machines, and computer hardware and software. As a condition of providing the above listed communications methods, the City places certain requirements and restrictions on their use. This policy addresses electronic mail.

III. PUBLIC RECORDS ACT / LEGAL CONSIDERATION

E-mail is a business tool which shall be used in accordance with generally accepted business practices and current law reflected in the California Public Records Act to provide an efficient and effective means of intra-agency and interagency communications. Under most circumstances, communications sent by email are subject to public disclosure under the Public Records Act or by litigation.

IV. E-MAIL PRIVACY

Since the computer and e-mail systems are the property of the City of Redondo Beach and provided for business purposes, users shall have no right or expectation of privacy or confidentiality in any e-mail message created, sent, received, deleted or stored using the City e-mail system. Management, supervisors and staff performing electronic discovery shall have the right to review and produce any e-mail message created, sent, received, deleted, or stored within the City's E-mail system.

V. POLICY

E-mail messages transmitted through the City's electronic mail system shall primarily support City business functions and the performance of official duties. Limited incidental personal use is permitted provided that it:

- does not interfere with employee productivity or City operations,
- does not incur additional costs to the City, and
- does not give the appearance of representing the City for non-City matters.

All official City business must be conducted exclusively through City-authorized communication platforms (e.g., City e-mail systems, approved collaboration tools) and not via personal e-mail or messaging accounts, except where explicitly authorized by the Director of Information Technology. Only the Information Technology Department may purchase, install and/or configure City-authorized communications platforms.

Upon separation from the City, access to City e-mail systems will be terminated and may only be restored with the written approval of the Director of Information Technology.

It is strongly advised that city e-mail accounts (e.g., *@redondo.org*, *@redondo.gov*) not be used as a personal identity or contact address for non-City business activities, including but not limited to:

- personal banking or financial accounts,
- consumer purchases or subscriptions,
- payment of personal utilities, rent, or mortgage, or
- registration for personal services, memberships, or government programs unrelated to City employment.

Those E-mail messages which are intended to be retained in the ordinary course of City business and recognized as official records by California Public Records Act, should be stored in an electronic file folder outside the e-mail system, e.g., on your P: (personal) drive, S: (departmentally shared) drive, Laserfiche, or printed and the hard copy filed in the appropriate subject file. Employees are responsible for identifying official records and copying or moving them to an official system of record (i.e Laserfiche) for long term storage. All other e-mail messages are considered transitory, and are not preserved in the ordinary course of business. The email system will automatically delete all emails after a period of 730 days.

All City policies (e.g., harassment policies) apply to electronic media. No electronic communications system, which includes e-mail, shall be used for personal gain or advancement of individual views. Solicitations for non-City business, or any use for personal gain, are prohibited. All electronic communications shall be appropriate and within City policy.

VI. VIOLATIONS

Any employee found to have violated this policy may have his or her access to email limited or revoked completely and may be subject to formal disciplinary action up to and including termination from City employment.

VII. EXCEPTIONS

There will be no exceptions to this policy unless approved by the City Manager.

VIII. AUTHORITY

By Authority of the City Manager

____
Mike Witzanksy

IX. ATTACHMENTS

N/A

ACKNOWLEDGEMENT OF RECEIPT AND UNDERSTANDING
OF E-MAIL COMMUNICATIONS POLICY

By signing below, I acknowledge that I have received a copy of the City of Redondo Beach Administrative Policy and Procedure regarding E-mail communications. I also acknowledge that I have read the policy, had the opportunity to have any questions answered, and that I understand the provisions contained in the policy.

Name: ______________________________________

Signature: ____________________________________ Date:________________

Supervisor: ______________________________________ Date:________________

CITY OF REDONDO BEACH		ADMINISTRATIVE POLICY AND PROCEDURES (APP)
Number: 04.05		**Subject: ARTIFICIAL INTELLIGENCE POLICY**
Original Issue: N/A	**Effective:** 3-16-26	**Category:** Information Technology
Supersedes: N/A		

I. PURPOSE

This policy establishes governance and operational standards for the use of Artificial Intelligence (AI) systems by the City of Redondo Beach ("City"). Its purpose is to ensure that AI technologies are used responsibly, securely, and transparently in support of City operations while protecting resident privacy and maintaining compliance with applicable laws and cybersecurity standards.

The goals of this policy are to:

- Provide clear guidance for City employees, contractors, and vendors who may purchase, configure, or use AI tools on behalf of the City.
- Define the approval process for new AI technologies, including mandatory review by the Information Technology (IT) Department.
- Ensure that AI systems are deployed in alignment with City cybersecurity, data protection, and privacy requirements.
- Maintain accountability, transparency, and human oversight in the use of AI.
- Prevent unauthorized or inappropriate use of AI technologies, particularly those involving sensitive data such as personally identifiable information (PII) or criminal justice information (CJI).

II. SCOPE

This policy applies to all City employees, departments, volunteers, consultants, and contractors who purchase, configure, develop, use, or manage AI tools or systems on behalf of the City.

This includes but is not limited to:

- **General-Purpose AI tools**, such as ChatGPT, Copilot, Gemini, Claude, and similar generative or conversational AI systems.
- **Department-Specific AI systems**, such as machine learning models used for data analysis, workflow automation, or decision support within a particular business process.

- **Embedded AI features** within other applications that perform predictive, analytical, or automated decision functions.

Employees must also remain aware that **many traditional or legacy software products now include AI features behind the scenes**, such as predictive typing, automated data analysis, or “smart” recommendations. Even if a tool appears conventional or familiar, if it includes any automated prediction, recommendation, or decision-making functionality, it is subject to this policy.

III. DEFINITIONS

Artificial Intelligence (AI):
A machine-based system that, for a given set of human-defined objectives, can make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use human- or machine-provided data inputs to perceive their environment, analyze information, and generate outputs that augment or replace human decision-making.

General-Purpose AI Tool:
Any broad or consumer-facing AI platform that is not developed or configured specifically for a City business function but can generate or analyze content for a wide range of uses (for example ChatGPT, Gemini, Copilot, Claude, or similar services). These tools are especially high-risk because data entered into them may be transmitted to third-party servers, used for model training, or disclosed outside the City’s control.

Department-Specific AI System:
An AI capability built or purchased for a specific operational purpose within a City department (for example predictive maintenance analysis, call routing, or permit review). If a software product performs automated tasks using models trained on data or that learn from user input, it qualifies as AI under this policy.

IV. POLICY STATEMENT

1. Authorization Requirement
   City staff are prohibited from using any AI system, service, or tool that has not been explicitly authorized in writing by the Information Technology Director.

   This includes free, public, or consumer versions of AI tools such as ChatGPT, Gemini, or Copilot, even when accessed with a personal account. These platforms are not secure for government use and often collect, analyze, and sell user data to third parties.

   The City will maintain a secure, enterprise-grade AI environment—TBD—as the sole approved general-purpose AI tool for City business. No other general-purpose AI platform may be used to generate, review, or analyze City data.

   This requirement applies equally to free or publicly available AI tools that:

- Do not require authentication or allow anonymous use;
- Allow login using personal accounts; or
- Are accessed through external websites or mobile applications not reviewed by the IT Department.

Staff should also remain aware that some approved or legacy applications may contain hidden or newly integrated AI components. Any new functionality labeled “intelligent,” “smart,” or “predictive” must be treated as AI and reported to IT for review before activation or use.

2. AI Tool Review Checklist and Product Selection
The IT Department will use a standardized AI Evaluation Checklist when reviewing any proposed AI system or product. This review process encompasses both tool authorization and product selection to ensure that the technology aligns with City standards and business needs.

The requesting department must provide to the IT Department:

- A clear written statement describing the business objective the department seeks to accomplish using AI;
- An explanation of why AI is necessary or beneficial for achieving that goal; and
- A list of alternative products or processes considered prior to requesting approval.

The IT Department’s evaluation will consider, at minimum:

- The type of data to be stored, transmitted, or processed.
- Whether data includes CJI, PII, HIPAA-protected, or confidential information.
- The vendor’s cybersecurity and privacy controls, including encryption, authentication, and access management.
- The product’s data retention, export, and deletion capabilities.
- Transparency and explainability of AI decision processes.
- Availability of audit trails, logging, and human oversight.
- Alignment with the City’s existing Information Security, Privacy, and Responsible Use policies.
- Compliance with CJIS and applicable federal, state, and local laws.
- Identification of any embedded or third-party AI services within the product that may process City data.

3. Procurement and Documentation
   All procurement or contract renewals involving AI systems must be coordinated with the IT Department and must include appropriate documentation (for example a vendor AI Fact Sheet or technical summary). Vendors must disclose any AI functionality within their products.

4. Incident Response and Reporting
   Any incident involving an AI system that results in the exposure, corruption, or misuse of City data must be immediately reported to the IT Department and handled under the City's cybersecurity incident response plan.

5. Police Department Considerations
   The Police Department shall maintain a separate, department-specific AI policy that aligns with this Citywide standard. That policy will include additional provisions for Criminal Justice Information Services (CJIS) compliance, investigative use restrictions, and law enforcement ethics.

6. Prohibited Uses
   AI tools shall not be used for:

   - Real-time biometric identification or surveillance without prior legal authorization.
   - Emotion recognition or sentiment scoring of individuals.
   - Fully automated decisions affecting employment, benefits, or public services without human review.
   - Social scoring or profiling of residents or employees.
   - Cognitive or behavioral manipulation of individuals.

7. Experimental Use and Proof of Concepts
   The City encourages departments to explore and experiment with AI technology in a responsible manner that promotes innovation while safeguarding City data.

   - Departments wishing to conduct AI-related experiments, pilots, or proofs of concept (POCs) must obtain prior written approval from the Information Technology Director.
   - Experiments and POCs must only use information that is publicly available or that the City would otherwise release under the California Public Records Act (CPRA).
   - If a department proposes to test AI technology using non-public, sensitive, or confidential data, a formal written contract or agreement must be established to ensure data protection, security, and compliance with applicable laws.

- IT reserves the right to halt any experimental AI use that poses a security or compliance risk.

V. GOVERNANCE AND RESPONSIBILITIES

- Information Technology Director
  - Serves as the City's AI Policy Authority.
  - Approves or denies AI tool usage requests.
  - Maintains the AI Evaluation Checklist and authorized tool inventory.
  - Coordinates reviews with the City Manager, Legal, and Department Heads as appropriate.
- Department Heads
  - Must ensure all departmental uses of AI are pre-approved by the IT Director.
  - Must maintain records of staff authorized to use AI tools.
- Employees and Contractors
  - Must comply with this policy and all related IT and security standards.
  - Must report suspected misuse or unauthorized AI activities to the IT Department immediately.
  - Must remain conscious of potential AI features in software tools they use daily and seek IT guidance before enabling or relying on them for City business.
  - Must only use the City-approved enterprise AI platform (TBD) for any general-purpose AI needs.

VI. PUBLIC RECORDS AND DATA PRIVACY

AI-generated content or outputs created in the course of City business are considered public records and must be retained or disclosed in accordance with the California Public Records Act (CPRA) and the City's record retention schedule.

All AI systems must comply with the City's Information Security Policy, Privacy Policy, and data classification standards to protect sensitive information.

VII. ENFORCEMENT

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, as well as potential legal or contractual consequences. Departments or vendors found to be in violation may have their AI privileges suspended pending review.

VIII. EXCEPTIONS

There will be no exceptions to this policy unless approved by the City Manager.

IX. AUTHORITY

By Authority of the City Manager

____
Mike Witzanksy

X. ATTACHMENTS

N/A

City of Redondo Beach Administrative Policy/Procedures 10.57 City Workplace Video Security Policy

Exhibit A – Camera Sites

Location	Quantity
City Hall	9
Fire Station 3	2
North Branch Library	10
Pier Skate Park	3
Police Annex Detectives' Bureau	4
Police Artesia SubStation	1
Police Evidence Warehouse	1
Police Main Station	42
Police Pier SubStation	4
Public Works Corporation Yard (Gertruda)	12
Public Works Parks Yard (Flagler)	4
Public Works Pier Yard (Pier Parking Structure)	2
Transit Center	54

CITY OF REDONDO BEACH		ADMINISTRATIVE POLICY AND PROCEDURES (APP)
Number: 10-57		**Subject:** Video Security Policy
Original Issue: 08-10-15	**Effective:** 3-16-25	**Category:** Risk Management, Safety and Information Technology
Supersedes: 08-10-20		

I. PURPOSE AND SCOPE

To set forth policy for the installation, operation, and maintenance of security cameras, monitors, and recording and storage equipment (“security systems”) to ensure security and safety on city-owned property.

II. GENERAL INFORMATION

A. The City may install and maintain security cameras capable of capturing, monitoring, and recording activity. An inventory of the current camera location sis provided in Exhibit “A.” This inventory shall be made viewable to the public on the City’s website.

B. The purpose of the installation of cameras is to deter crime, provide visibility, and to safely secure areas with a high probability of criminal activity or frequently host large group gatherings, and to protect certain high-value assets.

C. The City may install and maintain equipment capable of recording and maintaining data captured by security cameras pursuant to the authorization requirements of this policy.

D. All recordings made by the security systems shall remain the property of the City. Employees shall have no expectation of privacy or ownership interest in the content of the recordings.

III. INSTALLATION & PLACEMENT

The installation and/or removal of cameras shall be authorized by the City Manager, or designee, in consultation with the Chief of Police and Information Technology Director. The determination to install new cameras shall be based on the following criteria:

A. Crime Activity Metrics: Cameras may be installed in areas with a documented history of criminal activity including:

1. A pattern of repeated incidents at a particular location.

   Note: Regular analysis of incident reports and data should be conducted to identify trends and hotspots for criminal activity. This analysis will help determine the need for additional cameras, need for existing cameras to be removed, or the repositioning of existing cameras.

2. Response to or as a deterrent measure for particular types of crimes as designated by the Chief of Police with approval by the City Manager including reported incidents or threat of vandalism, assault, violent felony, etc.

B. Crime Prevention: Cameras may be installed in areas identified as high-risk for potential criminal activity to serve as a deterrent. Factors to consider include, but are not limited to:

1. Proximity to high-traffic areas or public spaces

2. Areas with limited natural surveillance or poor lighting

3. Locations with valuable assets or sensitive information

4. Locations where large crowds of people gather routinely

5. Vacant or abandoned properties

C. Voting Locations: Cameras may be installed in areas where election ballots are stored or processed and may only be engaged during an election cycle. These cameras shall only be used for the purpose of ensuring election integrity.

D. Review and Documentation: All decisions regarding the installation and placement of cameras must be documented, including the rationale and supporting data. Regular reviews should be conducted to assess the effectiveness of the cameras and adjust as needed. All new permanent (>90 day) security camera installations approved by the City Manager, or designee, shall be added to the City's inventory (10.57 Video Security Policy – Exhibit A) and made available for public viewing on the City's website.

E. Criminal Investigations: Nothing in this policy shall restrict the ability to install and maintain temporary (<90 day) video and audio recording devices for the purposes of criminal investigations conducted by the Redondo Beach Police Department or other law enforcement agencies.

IV. AUTHORIZATION TO OPERATE, ACCESS, AND MONITOR

A. Only authorized personnel may operate, access and monitor the security systems, and only in the manner specifically authorized. An internal list of authorized individuals shall be maintained by the Information Technology Department. Authorization may be provided as follows:

1. The City Manager, or designee, may authorize any employee of the City to operate, access, or monitor the security system, and such authorization is limited to the specific authorization given by the City Manager.

2. The Chief of Police may authorize any employee within the Police Department to operate, access, monitor and/or access recordings from the security system.

3. The Information Technology Director may authorize any employee within the Information Technology Department to incidentally access the security system for the purpose of system administration, troubleshooting or support.

B. Authorized personnel shall ensure that monitors and recordings of the security system are not visible or audible to unauthorized individuals.

V. PRIVACY

A. Restricted Areas: Security cameras must not be installed in areas where individuals have a reasonable expectation of privacy, such as private offices, restrooms, locker rooms, and other similar locations.

B. Data Protection: All video recordings must be stored securely to prevent unauthorized access, tampering, or loss. Appropriate measures must be taken to ensure the confidentiality and integrity of the recordings.

C. Review and Compliance: Regular reviews must be conducted to ensure compliance with privacy considerations and to address any concerns or issues that may arise.

D. Facial Recognition: Facial Recognition shall not be enabled unless approved by the City Council as a feature of the surveillance system, or temporarily in response to significant and/or active criminal threats for emergent public safety purposes as approved by the City Manager, Chief of Police and Information Technology Director.

E. Audio: Audio recording shall not be enabled outside of the Jail and Police Interview Rooms unless temporarily in response to significant an/or active criminal threats for emergent public safety purposes as approved by the City manager, Chief of Police and Information Technology Director or as required by law.

VI. RETENTION AND RELEASE OF RECORDINGS

A. Security System recordings shall be maintained for no longer than 60 days and in compliance with city, state and federal law.

B. Security Systems recordings may be released in compliance with a public records request, if permitted, by the California Public Records Act.

VII. EXCEPTIONS

There will be no exceptions to this policy unless approved by the City Manager.

VIII. AUTHORITY

By Authority of the City Manager

____

Mike Witzanksy

IX. ATTACHMENTS

A. Exhibit A – Camera Descriptions List