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