ADMINISTRATIVE REGULATION

Office of the City Administrator

Number	**AR 605**
Sections	**1 - 8**
Effective Date	**May 18, 2017**
Responsible Department	**Information Systems**
Review Date	**April 2019**

SUBJECT: Computing Resource Use

1. **Purpose:** This policy governs the operation and/or use of the City of Huntington Beach's information technology resources including, but not limited to, computers and computing systems, networks, software, internal and external e-mail, the Internet and Intranet. This also encompasses communications-related tools and other electronic devices/media such as tablets, smart phones, desk phones, cell phones, pagers, fax machines, copiers, printers, and voice mail, collectively referred to as information technology systems.

2. **Authority:** Section 401 of the Huntington Beach City Charter.

3. **Application:** This policy applies to all elected and appointed officials; employees (regular, extra-help, and temporary); contractors; volunteers; and other individuals who are provided access to the city's information technology, collectively "users." Third parties should only be provided access to the city's information technology as necessary for their business purposes with the city and only if they agree to abide by all applicable rules.

4. **Definitions:** For the purposes of this policy, the following definitions shall apply:
   - **4.1. Authorized User** - A city employee, or any person who has signed the Policy Agreement Declaration (attached) and is approved to utilize the specific system as part of their assigned official duties including, but not limited, to full or part-time employees, elected and appointed officials, volunteers, contract support personnel, and consultants.
   - **4.2. Authorized City Representative** - Each user's respective department head or the Chief Information Officer as appropriate.
   - **4.3. Cloud** - Any service/resource accessed from the Internet which provides data storage, computing services, servers, and other technology infrastructure.
   - **4.4. Confidential Information** – Information of a sensitive nature intended for recipients with a business need-to-know that may include, but is not limited to, personal content such as medical, recruitment, disciplinary, and performance information; attorney-client privileged communications; and other protected information. Unless exempted by law, some types of confidential information may be subject to legal inspection and/or disclosure requirements.
   - **4.5. E-Mail** - Any computerized system or software designated for the transmittal of written messages. Any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of communication across computer network systems between or among individuals or groups. Also included are services such as list servers, electronic bulletin boards, news groups, social media sites and instant messaging applications.
   - **4.6. Tablet** - A hand held, general-purpose computer with touch-screen capabilities.

5. **Policy:** It shall be the policy of the City of Huntington Beach that the use of all electronic media including city computers and tablets, internal and/or external e-mail, and/or access to the Internet or Intranet, shall be for job-related purposes.
   - **5.1.** Information technology systems are the sole property of the city. The city reserves all rights, including termination of service without notice, on all systems that it owns and operates. The city may restrict access to its systems without prior notice and without consent of the user. This policy shall not be construed as a waiver of any rights of the city, nor shall it conflict with applicable law.
   - **5.2.** The city, as provider of information technology systems, reserves the right to specify how the city's computing resources will be used and administered to comply with this policy and other city rules, policies, resolutions, and ordinances. This includes cloud as well as on premise systems.
   - **5.3.** The city may conduct reviews of the content of messages and files stored on network drives and web sites visited on the Internet, including random reviews, when in the exercise of its business judgment the city determines that it would be prudent to do so. The city further reserves the right to inspect, repair, service, and remove non-city-business files from all servers and workplace computers. The city reserves the right to review and disclose all information transmitted through these systems. The city may control access to its systems in accordance with the laws of California and the United States and the policies of the city. The city reserves the right to access all information stored on all city systems for any reason.
   - **5.4.** The information sources accessible via the Internet are worldwide and constantly growing in kind and number. The city reserves the right to restrict access to any of these sources if/when, at its sole discretion, the city determines a source is not necessary to facilitate city business. Restriction of a specified source does not imply approval of other non-restricted sources. Employees are prohibited from intentionally accessing any Internet sites that are discriminatory or offensive in nature or promote or advocate any form or type of discrimination. Employees are prohibited from posting personal opinions on the Internet using the city computer system's access without the City Administrator or his/her designee's approval. Any attempt to access a website that has been filtered by the network website filtering software, or any attempt to bypass the city network filtering measures by the use of software or hardware designed for the purpose of bypassing city filtering measures, is prohibited. Should the need arise to access a filtered/prohibited website, the employee should contact his/her supervisor and gain official authorization to have the Chief Information Officer allow the necessary access for the prescribed period of time.
   - **5.5.** Employees are forbidden from disabling or circumventing any computer-related security measure unless authorized by Information Services.
   - **5.6.** The city may suspend without notice information technology system privileges of a user for reasons relating to suspected violation of city policies; contractual agreements; or local, state, or federal laws. This includes, but is not necessarily limited to, instances of employee termination, investigations of information technology systems usage misconduct, or when the user is deemed to represent a threat to any component of the systems. Access will be restored when deemed appropriate by the city considering the circumstances surrounding the suspension.

6. **Procedure:**
   - **6.1.** City computers or information technology systems shall only be used for purposes relating to achieving the city's mission and shall not be used for personal business except as provided herein. Computer and communication systems are business tools to be used in accordance with generally accepted business practices; current laws including, but not limited to, the California Public Records Act; and consistent with the city's other policies including, but not limited to, the city's Document Retention Policy.
   - **6.2.** Information received or transmitted by any computer or communication system, whether deleted or not, may be logged, recorded, or otherwise monitored and is subject to disclosure based on the provisions of the Public Records Act and/or approval of the City Attorney.
   - **6.3.** E-mail shall not be used as a permanent storage medium. E-mail will be maintained on the city's e-mail server equipment or back-up media for 90 days. Calendar items will be maintained for 365 days. Automatic and manual archiving of e-mail will not be permitted. Network and local drive storage of e-mail files, other than outlined in section 6.4, will be disabled.

6.4. Unless exempt from disclosure under other applicable provisions of the Public Records Act, (personnel files, attorney-client communications, deliberative process, etc.), the user is responsible for insuring that e-mail with content that is subject to the city's Record Retention Schedule is placed in the appropriate subject folder, either electronically or in hard copy, for retention as per the schedule.

6.5. To protect against security threats and legal liability, e-mail communication must be handled in the same manner as a letter, fax, memo, or other city communications. All e-mail messages distributed through the city's e-mail system are considered city property. E-mail messages may not contain content that may be considered offensive or disruptive unless work related. This includes, but is not limited to, obscene or harassing language or images; racial, ethnic, political, sexual, or gender-specific comments or images that one may find offensive. Some city department employees may be able to send and receive such messages due to the nature of their work – for example, Police Department or City Attorney staff.

6.6. E-mail, either internal or external, shall only be used for purposes related to achieving the city's mission and shall not be used for personal messages or personal business. The exception for those authorized to send and receive outside e-mail would be short and infrequent messages; for example, to arrange or confirm appointments, correspondence with other governmental agencies, inform family of work hours or overtime assignments, etc., as long as it does not interfere with city business or job performance. Use of e-mail must be in accordance with all other information technology systems policy and procedures.

6.6.1. Examples of acceptable, incidental personal use of city information technology include:

- E-mail to notify family of a schedule change when an employee traveling on city business is delayed due to official business or a transportation delay.
- An employee is required to work overtime without advance notice and e-mails to advise his/her family of the change in schedule or to make alternative transportation or child care arrangements.
- An employee exchanges e-mail with family members (or those responsible for them, i.e., a school or day care center) to make certain of their well being and/or safety.
- The employee e-mails businesses that can be reached only during normal working hours, such as a local government agency or a physician.
- An employee e-mails businesses in the area to arrange for emergency repairs to his or her residence or automobile.

6.6.2. Employees should check with their supervisor if in doubt about the appropriateness of a personal e-mail or other use of information technology systems.

6.6.3. Personal use of the city's information technology systems is at the user's own risk and may be accessed, reviewed, copied, deleted or disclosed by the city.

6.6.4. Allowed personal use does not include:

- Usage for private gain, or in connection with compensated outside work, game playing, stock trading, browsing social media sites or chat rooms.
- The city does not permit use of city information technology systems for political or religious activities; sending messages or information that is in conflict with local, state, or federal law; applicable regulations of the network being used; city policies, rules, or procedures; unauthorized attempts to access data or break into any city or non-city system, and theft or unauthorized copying of electronic files or data.
- Harmful activities such as, but not limited to the following, are prohibited: creating or propagating viruses; disrupting services; damaging files; and intentionally destroying or damaging equipment, software, or data belonging to the city.

6.7. All messages from city information technology systems must appropriately identify the sender. Information technology systems may not be used to intentionally misrepresent one's identity. E-mail shall not be sent under another user's name without authorization. Another user's e-mail shall not be read unless there is a city purpose for doing so and is authorized by a supervisor. No previously sent e-mail message shall be changed without authorization from the original author.

6.8. Unless specifically authorized, no postings may be made to any social media site in the city's name.

6.9. Intellectual property (including but not limited to computer software, movies, books and music) is protected by copyright and is not to be copied from, into, or by using city-computing facilities, except as permitted by law or by the contract with the owner of the copyright. No software may be installed, copied, or used on city resources except as permitted by the owner of the software and the express permission of the Information Services staff.

6.10. No information technology systems equipment or software is to be purchased without the review and approval of the Information Services Department.

6.11. No personally owned hardware or software is to be used with or installed on any city computer resource without the review and approval of the Information Services Department.

6.12. Access to city information technology systems equipment and resources by recognized employee organizations is allowed consistent with this policy's references to non-work uses and any provisions in an applicable Memorandum of Understanding. Access shall be authorized only to the extent that union business is limited to those lawful activities that pertain directly to the employer-employee relationship and not such internal organization business such as soliciting membership; campaigning for office and elections; and shall not interfere with the efficiency, safety, and security of city operations. Employee organizations, and those representing them, shall have no greater access to use of computer resources than employees of the city. Use of city information technology systems to communicate between union representatives and city representatives is considered city business and shall be allowed during regular duty hours. Union use of the city's information technology systems is at the user's own risk and may be accessed, reviewed, copied, deleted, or disclosed by the city.

6.13. Users will ensure that all information technology systems assets: computer, monitors, laptop computers, tablets, printers, and other devices that are assigned to or regularly used by them, are maintained and used in a manner consistent with their function and such that the possibility of damage and/or loss is minimized. Whenever possible, all portable computing equipment: laptop computers, tablets, or other handheld computers, will be maintained under the direct supervision of the user that they are issued to. The equipment must never be left unattended in locations such as airports and hotel lobbies. When equipment must be left unsupervised, it must be made as inconspicuous as possible. Whenever practical, the computer shall be secured with the supplied security device(s).

6.14. Users are expected to report unauthorized access, including unauthorized access attempts or other improper usage of city computers, networks, or other information processing equipment. If a user becomes aware of a security or abuse problem with any city computing resource, including violations of this policy, the user must take immediate steps as necessary to ensure the safety and security of information resources by contacting your immediate supervisor and/or the Chief Information Officer.

6.15. Due to security/infection risks, Instant Messaging (IM) services, other than those provided by the City, including, but not limited to, SnapChat, WhatsApp, Facebook Messenger, MSN Messenger, AOL Instant Messenger, and ICQ, for example, may not be used on city computers.

6.16. Whenever an official or employee possesses confidential information, the official or employee has an obligation to take all reasonable and necessary steps to protect the confidentiality of the information and minimize the likelihood of inadvertent transmission of the confidential information to unintended recipients. If an official or employee has any question regarding the implementation of this section, contact the City Attorney's office. Employees must exercise caution when creating or transmitting city business information electronically. Confidential information may not be transmitted to employees or other individuals who are not authorized to receive such information. E-mail which contains confidential attorney-client information may not be disclosed to non-city personnel, except by the City Attorney's office, unless so authorized by the City Administrator or his/her designee, or as required under law. If an employee is unsure as to whether a communication is authorized, it is the employee's responsibility to inquire with their supervisor or the City Attorney as appropriate.

6.17. If it becomes necessary to send confidential information to an external location, contact the Information Services Department to arrange suitable encryption and/or a transport mechanism.

6.18. Employees may request permission to have remote access to the city's information network. Permission will be granted on a case-by-case basis by their department head. Employees with permission will work with the Information Systems staff for training on using their access. Any remote

access to the city's network is strictly for business-related purposes and is not to be shared with any individuals who are not employed by the city.

6.19. Computers should be locked via the operating system, either manually each time users leave their desks for any period of time, or automatically using a password-protected screen saver. At the end of the workday, employees must logout and turn the monitor off. The computer is to be left running to receive updates over the night. Information Services staff may ask users to remove their screen saver passwords in order to perform installations, diagnostics, repairs, replacements, upgrades, or maintenance. Once completed, the user is to immediately change it back to a unique and secure password.

6.20. When a permanent or temporary employee or on-site contractor requires access to a city computing resource, the department in which the employee resides completes the *Information Services Add/Move/Change form* on the Surfnet Forms & Templates section and sends it to the Information Services Help Desk.

6.21. When an employee is separated from service, the following steps are taken:

- Information Services will immediately disable the separated employee's remote access capability.
- If the department head has not already requested and received the employee's password, he or she will obtain the employee's password from Information Services.
- The department head or his/her designee will make a timely inspection of the employee's files and copy any files from e-mail and network drives which the department wishes to retain.
- Ten working days after separation, Information Services staff will disable the employee's account and will remove e-mail and files contained in the city network unless requested to do otherwise by the department head. Back-up storage of these files will be retained offline.

7. Procurement:

7.1. Procurement of computer equipment, software, or telecommunication products, including phones and cellular phones, shall be procured through an e-mail request to the Information Services Help Desk. Such requests will go through the standard technology purchasing process as posted on Surfnet. With the exception of Information Services staff, city procurement cards, credit cards, or petty cash shall not be used to purchase these items.

7.2. Information technology consumable items: toner cartridges, including diskettes, zip disks, CDs, DVDs, tape cartridges, flash drives, and paper, do not require Information Services Department review and approval.

8. Violations:

8.1. Violation of any provision in this policy will be reviewed on a case-by-case basis and may result in revocation of privileges, suspension, termination, and/or criminal prosecution. Failure on the part of any contractor, consultant, or non-employee to comply with the provisions of this policy will constitute grounds for revocation of privileges, termination of their contract, and/or criminal prosecution.

As a condition of using any the city's computing resources, all users must fill out and sign the attached Policy Agreement Declaration.

Behzad Zamanian, Chief Information Officer

Approved As to Form

Fred A. Wilson, City Manager

City of Huntington Beach
Computing Resource Use
Policy Agreement Declaration

DECLARATION BY THE EMPLOYEE:

The undersigned employee declares that:

a. He/she has been given the time needed to read and has, in fact, read the Computing Resource Use Policy in full;

b. An authorized City representative has offered to provide him/her, if so required, with information and explanations pertaining to this Policy;

c. Each and every one of the provisions of this Policy is legible;

d. An authorized City representative has given the employee a copy of this Policy.

EMPLOYEE'S COMMITMENT

The undersigned employee, as an authorized user, commits and agrees to:

a. Follow all provisions of this Policy;

b. Promote the spirit and the letter of this Policy;

c. Become familiar on a regular basis with any revisions or amendments to this Policy, as soon as the revised or amended Policy is made public, via posting on Surfnet or e-mail, and follow all provisions of the revised or amended Policy.

ACKNOWLEDGMENT

I have read the Computing Resource Use Policy (AR 605) and understand its provisions. I understand that use of the City's computer system, in any capacity, is a privilege and not a right. I understand that I have absolutely no right to privacy in any of the City's computer systems, ID's, files, etc., and that any materials that I have created, saved, downloaded, erased, etc., are subject to search and review by my employer. I accept responsibility for the appropriate use of City computer resources, including all computer systems, network systems, Internet, and Intranet web sites, or other data processing equipment owned by the City, as well as remote computers or computer systems when used to access the City computer resources as outlined in the Computing Resource Use Policy. I understand that use of City computer resources in violation of the Computing Resource Use Policy may result in employee discipline and/or the cancellation or restriction of user privileges. I agree to report any use, which is in violation of the Computing Resource Use Policy, to Information Services or to management.

THIS SECTION TO BE COMPLETED BY THE EMPLOYEE			
Agreement to the above:			
Employee's Name ***(Print)***	Signature	Phone	Date