CITY OF AVALON
Internet, Email, Computer Use, and Information Technology Security Policy

A. INTRODUCTION & PURPOSE

The City of Avalon encourages the use of electronic communications to share information and knowledge, in support of the City's mission and to conduct City business. The purpose of this policy is to outline the acceptable use of computer and other technological equipment at the City. This policy is intended to protect the City and its employees, as the inappropriate use of City equipment can effectively create exposure to virus attacks, compromise the network and its systems and services, and potentially create unintended legal issues.

The City is committed to protecting its employees, contractors, consultants, temporary employees and Council members. As such, this policy is not intended to impose restrictions that are contradictory to the established culture of openness, trust and integrity throughout the organization and with the public.

This policy is a living document and may be modified at any time by the City, subject to final approval by the City Manager and any modifications will be communicated to employees within a reasonable timeframe.

B. SCOPE

This policy is effective for all employees, contractors, consultants, volunteers, reservists, temporary employees and Council members and is applicable to internet/intranet related systems, computer equipment, software, operating systems, storage media, network accounts, email accounts, mobile devices and all other technology related equipment ("City Equipment") owned or leased by the City.

C. STATEMENT OF RESPONSIBILITIES

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

a. Manager Responsibilities

Managers and supervisors must:

- Ensure that all appropriate personnel have read, signed, and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

b. Information Technology Responsibilities

The Information Technology staff or designee must:

- Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.
- Provide periodic updates to reflect any changes in technology or copyright laws.

- Perform a system risk assessment annually that identifies threats and vulnerabilities on the City network.
- Install the latest security patches for all software and operating systems within 3 weeks of the patch being released by the vendor.

D. GENERAL USE AND OWNERSHIP

All City Equipment is the property of the City and to be used for business purposes in serving the interests of the City and of the public in the course of normal operations. City employees and officials shall not use City time, City funds, City facilities, equipment, or supplies for personal use or personal gain. This includes computers, internet access, and email. These resources are provided for City business only. While the City desires to provide a reasonable level of privacy, users should be aware that the data they create on City Equipment remains the property of the City. Because of the need to protect the City Equipment, management cannot and will not guarantee the confidentiality of information stored on any network device or file server belonging to the City. Even information that is "deleted" may still be accessible. Moreover, courts have been unwilling to find that employees have any reasonable expectation of privacy when an employee voluntarily places information onto a public agency's equipment. All City records, regardless of media or format and including e-mail messages and other electronic records are governed by the requirements of the California Public Records Act (CPRA). Requests for information under the authority of the CPRA that involve e-mail messages and/or attachments should be handled in accordance with standard City and departmental policies. Therefore, employees should be cautious when placing information on City owned equipment.

Furthermore, when employees use their own personal items, such as a cellular telephone or laptop at work, and gains access through the employer's internet to the server, the employer will be able to access the information that is in storage in the same way it can when employees use the employer's computer AND those same personal items may become subject to a CPRA request.

Attorney-Client Privileged Communications and Attorney Work Product - Some messages sent, received, or stored on the City e-mail system will constitute confidential, privileged communications between the City and its attorneys. Some messages may be subject to the attorney work product doctrine as well. Attorney-client communications and attorney work product should never be forwarded without consulting both the City Manager's Office and the City Attorney's Office.

E. DESKTOP AND NETWORK SECURITY

This Policy is intended to ensure the integrity and availability of data and resources through the use of effective and established Information Technology security processes and procedures. The following shall be effective for all applicable City equipment:

1. All PCs, laptops and workstations should be secured with a strong password to secure your information and accounts should not be shared among users. Passwords should have at least eight characters and include uppercase and lowercase letters, numerals and special

characters. Authorized users are responsible for the security of their passwords and accounts. It is important to keep different passwords for different accounts. This will reduce the chances that if one password fails your other accounts will be vulnerable as well. Do not use the same passwords for accessing work systems on any other accounts. System level and user passwords shall be changed yearly and the financial system password shall be changed every six months.

2. All PCs, laptops, servers and workstations used by an employee that are connected to the City's network, whether owned by the employee or the City, shall be continuously executing the City's approved virus-scanning software with a current virus database, unless overridden by the City's Information Technology designee. It is every employee's responsibility, to the best of their ability, to prevent viruses of all types from entering the City's network environment. A firewall is a software program or hardware device that filters the inbound and outbound traffic between your network or computer and the Internet. A firewall is a very valuable tool to protect your data and your computers. Firewalls can block intruders and unwanted traffic from getting into your computer. Employees shall make sure the firewall is always enabled on these devices. Employees are expected to exercise good judgment and use the following guidelines to prevent potential virus issues:

a. Employees must use extreme caution when opening email attachments received from unknown senders which may contain viruses, email bombs or Trojan horse code. Delete these attachments immediately then double delete them by emptying your Trash folder. Should the user suspect a questionable email, the Information Technology designee should be notified immediately to further prevent these types of files from entering the network.

b. Misaddressed e-mail shall be sent back to the original sender with a message that the message has been misaddressed, and the original deleted.

c. Delete spam chain and other junk email without forwarding. While it may be difficult to spot some phishing attempts, it's important to be cautious about all communications received, including those purported to be from "trusted entities" and be careful when clicking on links or attachments contained within those messages. Additionally, do **not** respond to any suspicious emails and do not open attachments contained in those messages. The scam typically attempts to entice email recipients into clicking on a link or opening an attachment that results in malware being downloaded onto your computer.

d. Never download files from unknown or suspicious sources and always keep your systems and software up-to-date. System and software vendors often find vulnerabilities that they fix in the latest update. Computers not updated, are left open to attacks via these vulnerabilities. Be cautious about devices that don't belong to you that you let connect to your equipment, as you cannot be sure that they are properly protected. Set programs and systems to auto-update to avoid missing a critical update. This includes your operating system, office suite, Adobe, media players, browsers, and other programs that can access the Internet. If you are unsure whether your system has the correct settings please contact the City's Information Technology designee.

e. Always run the City standard supported anti-virus software. The City's Information Technology designee will provide support as needed. Anti-virus programs can stop viruses, worms, and other malware. Anti-spyware programs can stop malware that perform certain behaviors such as pop-up advertising, collecting personal information, or changing the configuration of your computer. It is important to keep these up-to-date by keeping the license active and the program set to auto-update.

F. DATA STORAGE AND BACKUPS

All employee data files, including, but not limited to Word, Excel, PDF, Access, PowerPoint files, etc., shall be stored on the City's shared drives O: or U:. The Desktop area is intended for temporary storage and not meant to be a permanent storage area as there are no guarantees this data will be backed up on a regular basis.

The City's Information Technology designee is responsible for ensuring data backups occur on a regular basis. Full backups of all data files and server operating systems shall be performed on a weekly basis, where incremental backups of the same will occur on a nightly schedule.

G. UNACCEPTABLE USE

Under no circumstances are employees of the City authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City Equipment. The following activities which are considered unacceptable use and are prohibited, include, but are not limited to:

System/Network/Internet Activities

1. The intentional display or transmission of electronic mail and information systems of the City are not to be used in a way that may be disruptive, offensive to others, or harmful to morale. For example, the City prohibits the display or transmission of sexually explicit images, messages, jokes, cartoons, or any transmission or use of e-mail communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, color, sex, sexual orientation, age, disability, religious or political beliefs, or any other characteristics that may be protected by civil rights laws.

2. The intentional violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to the installation or distribution of pirated or other software products that are not appropriately licensed for use by the City.

3. The intentional unauthorized copying of copyrighted material, including but not limited to digitization and distribution of photographs from magazines, books or other copyrighted sources. Copyrighted music and the installation of any copyrighted software for which the City or the end user does not have an active license is strictly prohibited.

4. The intentional introduction of malicious programs into the network or server, e.g. viruses, worms, Trojan horses email bombs, etc.

5. Revealing account passwords to others or allowing use of account by an unauthorized person(s). This includes family and other household members when work is being done at home.

6. Using City Equipment to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the City's jurisdiction.

7. Making fraudulent offers of products, items or services originating from City Equipment or a City account; and/or using City Equipment or accounts for commerce.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.

9. Port scanning or security scanning is expressly prohibited unless permission is obtained from the City's Information Technology designee.

10. Executing any form of network monitoring which will intercept data not intended for the employee unless this activity is a part of the employee's normal job/duty.

11. Circumventing user authentication or security of any host network or account.

12. Interfering with or denying service to any user other than the employee's host, for example denial of service attack.

13. Using any program, script, command, or sending messages of any kind with the intent to interfere with or disable a user's terminal session via any means, locally or via the internet/intranet.

14. Providing information about or lists of City employees or customers to parties outside the City without permission.

15. Copying, altering, modifying, disassembling, or reverse engineering the City's authorized software or other intellectual property in violation of licenses provided to or by the City.

16. Installing, uploading, or downloading unauthorized or unlicensed software, or any form of intellectual property created for the City, on a City PC, laptop or network server without a third party agreement or contract, and prior approval from the City's Information Technology designee.

17. Executing or downloading any non-business related internet program or file that utilizes excessive bandwidth on the network, i.e. Web radio, MP3 downloads, etc.

18. Performing Information Technology related tasks without prior approval from the Information Technology designee. This includes the setup and installation of new technology equipment that connects to the City's network and/or tampering with existing equipment.

19. Playing games or gambling, whether over the Internet or on a standalone computer.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of junk mail or other advertising material to individuals who did not specifically request such material, i.e. email spam.

2. The City's email system shall not to be used for the creation or distribution of any disruptive or offensive messages including, offensive comments about race, gender, disabilities, age, sexual orientation, , religious beliefs and practice, political beliefs or national origin, or any other characteristics that may be protected by civil rights laws,. Employees who receive any emails with this content from any City employee should report the matter to their supervisor immediately.

3. Any form of threats, bullying or harassment via email, telephone, paging or text messaging.

4. Unauthorized use or forging of email header information.

5. Solicitation of email for any other email address other than that of the poster's account with the intent to harass or to collect replies.

6. Creating or forwarding chain letters or other pyramid schemes of any type.

7. Posting the same or similar non-business related messages to large numbers of Usenet newsgroups, i.e. newsgroup spam.

8. Deleting email messages in violation of the City's existing Record Retention policy.

H. PERSONAL USE

Incidental and occasional personal use of the Internet as covered by this policy may be permitted at the discretion of the employee's Department Director or City Manager. However, such use shall be treated the same as official use, and thus, the employee shall have no expectation of privacy when using City systems for personal use. As such, personal use is subject to the same access and review rights as any other use of these systems.

I. EMAIL SIGNATURE

The City requires all staff members to use a standardized email signature, as approved by the City Manager, in all internal and external communication related to the City. This signature gives recipients an understanding of the sender's name and position in the City, while maintaining credibility. In addition, this signature represents the City and helps maintain a clean, cohesive brand.

J. BLOGGING/SOCIAL MEDIA

Blogging is an online journal that is frequently updated and intended for general public consumption. Personal blogging by employees using City Equipment is subject to the terms and restrictions set forth in this Policy and any City's Social Media Use and Public Outreach Policies. Certain employees, officers, and designated contractors who, as part of their job responsibilities and requirements, are authorized to speak on behalf of the City in their official capacity. Limited and occasional use of City Equipment to engage in personal blogging is acceptable provided it is done in a professional and responsible manner, does not otherwise violate any City's policies, is not detrimental to the City's best interests, nor does it interfere with any employee's regular work duties.

1. Official content posted to blogging sites should contain links directing users back to the primary City websites for in-depth information, forms, related documents or on-line services designated to facilitate business with the City. This Policy applies to all City of Avalon ("City") employees, officers, and designated contractors who, as part of their job responsibilities and requirements, are authorized to speak on behalf of the City in their official capacity.

2. Employees shall not engage in any blogging, both on and off duty that may harm or tarnish the image, reputation and/or goodwill of the City and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments of others based on their race, national origin, color, sex, sexual orientation, age, disability, religious or political beliefs, or any other characteristics that may be protected by civil rights laws, when blogging or otherwise engaging in any conduct prohibited by the City's Non-Discrimination and Anti-Harassment policy.

3. Employees that engage in blogging in an unofficial capacity during their own time may not attribute personal statements opinions or beliefs to the City. In such cases where employees express a belief and/or opinion on a blogging site, employees may not expressly or implicitly represent themselves as an employee or representative of the City. Employees assume any and all risk associated with blogging.

K. REMOTE ACCESS TO CITY NETWORK

City employees and authorized third parties, vendors, etc. may use remote connections to gain access to the City's network as authorized by the Information Technology designee.

Remote access should be strictly controlled using a VPN (Virtual Private Network) and password authentication.

It is the responsibility of employees with remote access privileges to ensure a connection to the City's network is not used by non-employees to gain access to the system resources. Employees granted remote access privileges must remain constantly aware that the connections between their location and the City are literal extensions of the corporate network and that they provide a potential path to the City's most sensitive information. Employees and/or authorized third parties must take every reasonable measure to protect City assets.

L. NON-CITY ISSUED EQUIPMENT

Employees using non-City issued equipment that requires a wireless or direct connection to City Equipment or the network, is prohibited unless prior approval is obtained by the City's Information Technology designee.

M. TERMINATION OR CHANGE OF ASSIGNMENT

a. Return of Assets: When employees leave the City, all Information Assets remain the property of the City. Employees may not take such information when they leave, without the prior express written authorization of the City Manager.
b. Removal of Access Rights: Upon termination of said employees or vendors, the City shall automatically disable or delete accounts for said individual(s).

N. ENFORCEMENT

Any employee, contractor, consultant, volunteer, reservist or temporary employee found in violation of this Policy may be subject to disciplinary action, up to and including termination of employment or services.