AGENDA REPORT

CITY OF SAN CLEMENTE

City Council Meeting

Meeting Date: 9/6/2022 Agenda Item: 4J

Department: Information Technology
Prepared By: Brian Brower, IT Manager

Subject:
INFORMATION TECHNOLOGY POLICY AND PROCEDURE UPDATE

Fiscal Impact:
None.

Summary:
STAFF RECOMMENDS THAT the City Council approve and adopt City Policy 601-8-19 Use of Information Technology.

Background:
The City of San Clemente maintains a Policies and Procedures manual, which includes the major systems and procedures relating to the interaction of its organizational departments. The Policies and Procedures manual is intended to represent a unified and consistent approach to sound municipal government and is designed to provide public documentation describing overall policy, rules of procedure, and methods of operation.

Discussion:
A number of City Policies and Procedures pertain to the Information Technology Division. A core component of Information Technology best practices is the establishment, dissemination and enforcement of policies and procedures. Effective policies and procedures guide the use of technology to ensure a secure, reliable, and supportable environment. These policies provide a framework for the usage of technology, technical and security controls, and best practices in order to ensure the confidentiality, integrity and availability of the data at City of San Clemente.

Staff has identified a need to update existing Information Technology policies to align with best practices and has undergone a process of reviewing and updating existing policies, as well as developing new policies. Some existing policies have been revised, while others have been completely replaced. In addition, several new policies have been added which are not new ideas altogether, but rather memorialize best practices that are already being adhered to. The proposed policy updates have undergone a review and approval process involving the City's IT Steering Committee and the City Attorney's office.

Policy 601-8-19 represents a compilation of policy updates which define and regulate the acceptable use of the City's technology-related systems, including computers, tablets, mobile devices, telephones, software, electronic files, data, email, network and Internet systems, and establishes guidelines for use of these systems provided by the City to employees for the purpose of performing job functions. This policy will supersede Policy 601-8-17 (September 2, 2008), 1001-1-1 (July 1,

1992), 1001-1-3 (July 1, 1991), and 1001-1-5 (July 1, 1991).

Upon City Council approval, staff will be required to review and acknowledge these policies. In the future, these policies shall be reviewed by the Information Technology Manager on an annual basis and may be updated as needed with City Manager approval.

Plan and Policy Consistency:

This policy is consistent with the Information Technology Strategic Plan.

Recommended Actions:
Staff Recommendation

STAFF RECOMMENDS THAT the City Council approve and adopt City Policy 601-8-19 Use of Information Technology and authorize the City Manager to update as needed.

Attachment:
1. Policy 601-8-19 Use of Information Technology

Notification:
None.

POLICY AND PROCEDURE

Subject:	Use of Information Technology	***Index:***	Human Resources
		Number:	601-8-19
Effective Date:	September 6, 2022	***Prepared By:***	Information Technology
Supersedes:	1001-1-1, 1001-1-3, 1001-1-5, 601-8-17	***Approved By:***	

1. *PURPOSE:*

The purpose of this policy is to define and regulate the acceptable use of the City's technology-related systems, including computers, tablets, mobile devices, telephones, software, electronic files, data, email, network and Internet systems, and to establish guidelines for use of these systems provided by the City to its employees for the purpose of performing job functions.

The objectives of this Policy are:

- To maximize and ensure the efficient and effective use of the City's information technology resources;
- To maintain the integrity and security of computer based information and systems;
- To meet applicable federal and state laws and regulations regarding public access to information; and
- To protect the City from liability.

2. *ORGANIZATIONS AFFECTED:*

This policy applies to all City employees and officials, persons working as an agent of the City, contractors, vendors, volunteers, interns, and other authorized persons who use any Information Technology (IT) equipment or other communication device owned and provided by the city, who have been provided with City email accounts, or who are granted access to the City's network or computing resources.

3. *REFERENCES:*

City of San Clemente Employee Personnel Rules
California Public Records Act

4. *DEFINITIONS:*

4.1. "City" shall mean the City of San Clemente

4.2. "User" shall mean a city employee or official who is authorized to utilize the System

4.3. "System" shall mean and include the City's electronic data processing and communication systems. These include computers, printers, networks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the City. For example, IT Systems include departmental and city wide information systems, internet access, e-mail, desktop computers, laptop computers, servers, networking equipment, printers, scanners, PDA mobile devices, phones, cell phones and other devices supported by IT.

4.4. "Public record" includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.

4.5. "Record Retention Schedule" shall mean a document, adopted by the City Council, which identifies the period of time for which various types of records shall be retained.

5. *POLICY:*

5.1. Ownership

All electronic systems, hardware, software, temporary or permanent electronic files, electronic mail and electronic documents, and any related systems or devices are the property of the City. These include, but are not limited to, computers, tablets, telephones, mobile devices, network equipment, software, documents, spreadsheets, emails, and other electronic files which reside in part or in whole on any City electronic system or equipment. Any software, including databases, custom reports, graphics, or other work product developed while using a City resource or developed for use on the City network becomes the property of the City.

The City has the authority to inspect the contents of any city owned computing device and/or file(s) in the normal course of business and may request Information Technology staff to extract information, files, documents, email messages, etc., through authorization by the City Manager, City Attorney, or designee. Reasons for review include, but are not limited to, system hardware or software problems, general system failure, a legal action taken against the City, California Public Records Act Requests, suspected unlawful activity or violation of policy, or a need to perform work or repairs on technology systems.

5.2. Computer Usage

The City supplies computer hardware, software, systems and appropriate technology training to City employees in order to enable employees to perform their job duties effectively and efficiently. Computer hardware, software, and electronic equipment are provided to employees for the sole purpose of conducting the City's business.

Prohibited uses of City electronic systems and information include, but are not limited to, the following:

1. Illegal activities, including threats, harassment, slander, or defamation.
2. Transmitting messages or accessing content deemed sexually or racially offensive, obscene, discriminatory, lewd, sexually explicit, pornographic, defamatory, unprofessional, or otherwise objectionable.
3. Displaying, downloading, or distributing any hostile, offensive or sexually explicit material.
4. Personal commercial activities for profit or financial gain.
5. Soliciting, advancing or proselytizing for religious or political causes, commercial ventures, outside organizations, or other non-job-related solicitations.
6. Activity which could expose the City to liability or cause an adverse public perception.
7. Removing equipment, software or data from City premises without prior authorization.
8. Accessing, without a work-related need to know and authorization from management, any database or file containing confidential information, including but not limited to personnel records, financial records, or criminal histories, whether or not the confidential information is disseminated to any other person.
9. Executing any form of network monitoring that will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network, or account.
11. Using hardware or related computer equipment and software not authorized and/or owned by the City.
12. Manipulation of data files for the purpose of personal gain.
13. Any use that is inconsistent with City Policies and Procedures.
14. Storage, reproduction, or transmittal of any copyrighted files or information other than in accordance with the requirements and allowances of the copyright holder.
15. Launch of network attacks of any kind including port scans, DoS/DDoS, packet floods, replays or injections, session hijacking or interception, or other such activity with malicious intent.
16. Transmittal of malicious software such as viruses, Trojan horses, and worms.
17. Surreptitious installation of software or configuration changes to any device or application, or execution of key loggers, or other executable or active application or script.

5.3. Personal Use

Incidental personal use is acceptable unless it interferes with work duties or violates any stipulations within this Policy. Employees may occasionally use internet during breaks for personal use, provided such use does not interfere with job performance, consume significant amounts of time, distract other employees, does not potentially cause discredit to the City, does not result in personal profit or gain, and is done in a safe, professional and courteous manner. All other provisions of this policy are in effect when resources are used for personal use, including prohibited uses of City electronic systems and information contained in Section 4.2 of this Policy. The City reserves the right to filter, log, and/or monitor Internet usage by City employees.

5.4. Privacy

The use of the City's computer and/or electronic systems is not guaranteed to be under any degree of privacy. System support personnel have the right to access all files, documents, and records which are appropriate to accomplish their tasks. Managers have the right to access all files, documents, and records created by their department staff.

The City reserves the right to access and review all software programs, documents, electronic mail, notes, journal entries, or any electronic data created or stored on and/or sent over the City's computer network, including files or messages transmitted via e-mail and Internet access. Access may occur for reasons of, but not be limited to, situations indicating impropriety, violation of City policy, legal requirements, suspected criminal activities, suspected breach of electronic mail security, locating substantive information that is not more readily available by some other means, or for the performance of routine maintenance. Any material placed on the System is subject to inspection and copying at any time. Employees should not consider their Internet usage or email communications to be private.

Employees should be aware that any technology media or communication involving the City's technology resources are considered at all times to be City property, and may be considered public record subject to disclosure under the California Public Records Act or other lawful requests. The City shall comply with all lawful requests for information and obligations under federal and state law.

5.5. New/Departing Users

Access to the City's information and communications systems and equipment is controlled and administered by the Information Technology Division. The Information Technology section of a New Employee Onboarding Checklist must be completed and submitted to Human Resources prior to granting access for a new user of the City's information systems.

Upon the termination of an employee, the Human Resources Division shall notify the IT Division prior to the employee's final day of work. Employee access to IT systems shall be disabled at close-of-business on the employee's final day on the job. In cases where the employee is terminated without notice, IT shall be notified immediately so that access to City IT systems can be blocked.

5.6. User Accounts and Passwords

Each computer user will be assigned a unique user account and will set their own password subject to the City's password policy. The user is solely responsible for all actions taken while using his or her user account. Users should lock their computer when leaving their workstation unattended. Computers that are inactive for fifteen (15) minutes will be automatically locked. The employee must enter their password to unlock their computer.

Passwords are considered "confidential" and should not be disclosed to other users or any outside party under any circumstances. Users shall not reveal their password to any other person or allow any other person to login to a computer using their user account. Passwords shall not be left written down in any area within the City's facilities where they can be easily

accessed. If a password is written down on a piece of paper it must be shredded immediately after its use. The City's Information Technology (IT) Division does not store employee's passwords. If an employee needs to reset their password, they may submit a request to the Information Technology (IT) Division to reset their password, which will be tracked in the City's helpdesk system.

It is the responsibility of each employee to remember and safeguard his/her system passwords. The City network policy will force each user to change their password every 180 days. Passwords must meet the following criteria:

- The password cannot contain significant portions of the user's name
- Minimum of 8 characters in length
- Contain characters from three of the following four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numeric digits (0 through 9)
- Non-alphabetic characters (Ex. @ ! $ # %)

5.7. Hardware / Software Purchases, Licensing and Installation

All computer software and hardware purchases and installation must be coordinated through the Information Technology Division in order to assure that it meets standards that are compatible and supported by the current network infrastructure.

Equipment and software must be purchased from reputable, vendor-authorized resellers who can provide maintenance, warranty coverage or technical support services, and certified licensed software.

All hardware and software installations and upgrades on City workstations must be performed by authorized personnel. Employees may not install, relocate, or upgrade workstation hardware or software without the authorization from IT Division staff.

All software used on the City network must be legally licensed by the City and approved by the Information Technology Division.

No software may be downloaded or installed without the prior authorization and installation by the Information Technology Division.

The City and its employees shall abide by the terms of license agreements. City employees shall not duplicate, modify, or manipulate software licensed by the City. Software held by the City under a license agreement may not be supplied to an outside party unless the license agreement permits such use.

Employees are not authorized to install personally owned copies of software on City workstations. Use of commercial software not licensed by the City, but licensed to a City employee, may not be used on a City owned computer.

5.8. Use of Computer Equipment not owned by the City

Employees, consultants, and any other individuals are strictly prohibited from connecting personal laptops or any other computing devices directly to the City network, either directly or through the remote VPN portal, unless authorized by the Information Technology Division. The City provides guest wireless access in City Hall and other City facilities for connection to the Internet for devices not owned by the City.

Use of personal devices including USB devices such as flash drives, smartphones, music devices, etc., may not be used on a City owned PC or attached to any City owned network device without prior approval and authorization by the IT Division.

Authorized City employees may use their personal devices for limited work related tasks. Access from personally owned devices is limited to the City's email system, which includes remote access to email, calendar and contacts. Access to any other internal City network resources from personally owned devices is not permitted. Devices must meet standards and security requirements established by the Information Technology Division. The device should be current with a recent, supported operating system, which allows for the latest security patches to be in place. No personal device is authorized if it is "jailbroken" or programmed to bypass the manufacturer's restrictions put on the device.

City employees understand that electronic communications regarding City business are subject to the City's records retention policy, even if those electronic communications are or were created, sent, received or stored on a personally-owned electronic computing account or device.

The user must not store or access City information on a personally-owned device without authorization. When electronic communications that pertain to City business are received on a personally-owned email account or personally-owned device, the user must either (a) copy ("cc") the electronic communication from the personal email account or personally-owned device to the user's City email account or (b) forward the associated electronic communication to the user's City email account, no later than 10 days after the original creation or transmission of the electronic communication.

Users are required to delete all City data when replacing / decommissioning a personal device, when no longer using the personal device to support City duties, or when no longer continuing to work for the City. If a user replaces or upgrades a device, they are responsible for contacting the IT Help Desk to have the decommissioned device removed from the management system on its last day of service.

The IT Division will only provide support to personal devices for the following tasks:

- Configuration/access to City email account
- Connection to the City's wireless networks

The Information Technology department will not provide support to personal devices for the following:

- Configuration of personal email accounts
- Cellular network connectivity.
- Device hardware or software support.

5.9. Electronic Mail Systems

Electronic Mail and Internet systems enable employees to improve efficiency in the performance of job duties and to assist and facilitate business communications and work-related research. These systems are to be used in accordance with generally accepted business practices and current law (i.e. California Public Records Act). These services are for legitimate business use only in the course of employees' assigned duties.

5.9.1. City employees and persons working as an agent of the City, including contractors and elected/appointed officials, may be provided with City email accounts for the conduct of City business.

5.9.2. All messages transmitted over the City email system should be limited to those that involve City business activities or contain information essential to its employees for the accomplishment of business-related tasks.

5.9.3. Employees must use extreme caution when opening email attachments received from unknown senders. Email attachments from unknown senders may contain viruses or other malicious code. When in doubt, contact the IT Help Desk prior to opening this type of email.

5.9.4. All email communication from City Staff to City Councilmembers must be cleared through the City Manager's office before it is sent, and the City Manager should be copied on all correspondence to City Councilmembers.

5.9.5. To avoid Brown Act issues including serial meetings, City officials should avoid "replying all" to email communications when other City officials are copied to the email.

5.9.6. City personnel and elected/appointed officials should only use their City email account to conduct City business. The use of personal email accounts to transmit messages regarding City business is prohibited. If you receive an email that pertains to City business on your personal account, you shall either (a) copy ("cc") any communication from your personal account to your City email account; or (b) forward the associated email to your City email account no later than 10 days after the original creation or transmission of the electronic communication to ensure a copy exists in the City email system.

5.9.7. City personnel and officials understand that email regarding City business is subject to the City's records retention policy, even if the email is or was created, sent, received or stored on a personal electronic messaging account.

5.9.8. City personnel are expected to remember that e-mail sent from City email accounts is a representation of the City. All City personnel must use normal standards of professional and personal courtesy and conduct when drafting email messages. Email messages should be drafted with the same care and in the same manner as any communication printed on City letterhead.

5.9.9. Deletion of Material

Any material within the City's Email System may be considered public record subject to the same rules and regulations as paper-based communications. City email users may delete messages from their "Deleted Items" file, or any other email folder, when such material is deemed to be unnecessary for operational reasons. All deleted emails, including material "permanently" deleted and no longer visible to the users, shall be retained by the City's Email System for a two year period from the date sent or received. All emails, including items residing in the Inbox, Sent, Calendar Items, and any other system or user-created folders, shall be retained for a two year period. Following expiration of the two year retention period, all emails shall be automatically purged from the email system.

5.9.10. Email Retention and Public Records

The email system is intended as a medium of communication only and should not be used for long term storage or maintenance of documentation or official public records. However, the city does recognize that when retained in the normal course of business, email may be subject to applicable records retention requirements outlined in the City's Record Retention Schedule.

Emails typically fall into two basic retention categories:

1. *Emails that are retained within the email system for two years from inception or receipt*: General correspondence relating to City business that is retained in the normal course of business, shall be retained for two years as outlined in the City's Record Retention Schedule.

2. *Emails that are considered Public Records or must otherwise be preserved for a legally required time period greater than two years in accordance with the City's Record Retention Schedule*: Any email deemed to be a public record, that by the nature of its content must be retained longer than the limits outlined within this email policy shall be stored outside of the City's email system in an appropriate long term storage area. These items shall be either printed and filed in accordance with the City's Record Retention Schedule, or saved outside of the email system in the City's Electronic Document Management System (EDMS), or other designated platform for the long term storage of electronic records. Similarly, any email subject to any type of litigation hold shall also be stored in an appropriate long term storage area.

It is the responsibility of the end user to determine which of the two options listed above is appropriate for a particular email. If an email is a Public Record, the user is responsible for the preservation of the record for the legally required time period in accordance with the City's Record Retention Schedule.

To determine if an email qualifies as a Public Record or must otherwise be retained, individuals should apply the same criteria routinely used in determining the retention requirements for communications and documents. Questions about message retention should be directed to the City Clerk's Office.

5.9.11. Public Records Requests for Email

Upon approved requests, IT can search all email that is currently "live" on the City's email system. Live emails are defined as emails that currently exist in users' Inboxes, Sent, and Deleted Items folders, as well as any other user-created folders within the user's mailbox. Email records that reside within the live email system, and that are not exempt from disclosure by virtue of the Public Records Act, are subject to disclosure. The contents of email may be disclosed within or outside of the City without the employee's permission or knowledge.

In the event a Public Records Act request is received by the City seeking electronic communications of City personnel or officials, which specifies items that may be stored within personal devices or systems not owned or controlled by the City, the City Clerk's office shall promptly transmit the request to the applicable individuals whose electronic communications are sought. It shall be the duty of each City-affiliated individual within 10 days of receiving such a request from the City Clerk to promptly conduct a good faith and diligent search of his/her personal electronic accounts and devices for responsive electronic communications that reflect the public's business (and are not purely personal communications), and must then promptly transmit any responsive electronic communications to the City Clerk to review. City personnel, the City Clerk and the City Attorney will work in consultation to determine whether the responsive electronic communications produced from personal electronic messaging accounts and devices are related to the public's business and are disclosable under the Public Records Act. Failure of City personnel to comply with these required searches in response to a Public Records Act request may be subject to discipline.

5.9.12. Email Archives

Users who archive email files outside the live email system shall be responsible for the production of those documents in the event of a Public Records Act request.

Upon termination of employment, the IT division will archive the user's emails residing within the live email system. Archived email items will be retained for 2 years from the date they are sent or received, and are subject to discovery.

5.10. No City Representation

Only authorized employees may communicate on the Internet on behalf of the City organization. Employees may not express opinions or personal views that could be misconstrued as being those of the City unless they are acting in an official capacity. Employees may not state their City affiliation on the Internet unless required as part of their assigned duties.

5.11. Mobile Computing Device Use for City Business

For employees whose job duties require or benefit from working on an electronic device when located away from the office, the City may issue a City-owned device or authorize an employee to utilize a personally-owned device for City business. Users must protect the device at all times from loss, theft, or damage. In the event of loss, theft, or damage, the employee must notify the IT division so that appropriate action can be taken. In the event that a user is terminated or resigns from the City, the device must be returned to the City. At any time upon request, the Information Technology (IT) Division may require the user to provide any City-owned device for inspection.

Any employee that is issued a city device shall not install or uninstall any applications, or modify any security configurations, without prior authorization from the IT Division. These devices are for legitimate business use only in the course of employees' assigned duties.

If a mobile device covered under this policy cannot be located, the user is responsible for reporting the lost device to the IT Help Desk by the next business day after the loss. The IT Division will attempt to locate the device and may perform a remote “device wipe” to erase City data from the device.

5.12. Mobile Device Management Policy

The City may use a Mobile Device Management (MDM) software system that allows IT administrative control over city issued tablets, smartphones, and laptops. This system allows for management of passwords, remote connection settings, increased device security, control of allowed applications, and location of lost or stolen devices. This software may not be removed or tampered with while the device is being used for City business.

Download of applications may be restricted, or applications may be removed, if those applications are considered inappropriate, unrelated to City business, or they are considered a threat or significant risk to the City network environment.

From time to time, mobile device users may be asked to present their device to IT for a software update, or receive instructions on how to download and update themselves. Mobile Device users must promptly comply with these requests.

Mobile Devices are used as convenience and productivity enhancing tools. Due to their somewhat volatile nature, the data on these devices is considered as transient convenience

copies. Users are required to maintain a copy of any data that needs to be retained per City policy within a city file system other than local storage on the mobile device.

5.13. Mobile Access to Email

Only mobile devices that support Exchange ActiveSync technology for City e-mail synchronization are supported by the IT Division (Ex. iPhone/Android). Exchange ActiveSync mobile devices are designed to integrate with the City's email system and sync wirelessly without physical connection to City networks and do not require the installation of special software. Exchange ActiveSync maintains a synchronized copy of email system data such that all data is maintained within the City email system. For non-exempt employees, access to City Email from a personal computer or mobile device must be approved using the Remote Email Access form available on the City Employee Intranet. The request form must be signed by the employee's Supervisor and Department Head. Employees must protect their personal devices with a screen lock or password and should notify the IT Department immediately if the device is lost or stolen. The City is not responsible for troubleshooting or repair of non-City owned devices.

5.14. Public Records Requests and Mobile Devices

Any City-related electronic communication and any City-owned information stored on a City-owned or personally-owned electronic computing account or device may constitute a record subject to disclosure under the California Public Records Act (CPRA), the California Code of Civil Procedure, the Federal Rules of Civil Procedure, or other applicable statutes, regulations, or legal authorities. City employees and agents shall have no expectation of privacy or confidentiality in these records and shall cooperate with the City in producing them when requested as described in additional detail within the City's Electronic Mail Policy. Such cooperation includes conducting a good faith and diligent search of one's personal electronic messaging accounts and devices, as well as any City-issued electronic devices, for responsive electronic communications that reflect the public's business (and are not purely personal communications) in response to a Public Records Act request received by the City. This search must be completed within 10 days of receiving notice that a Public Records Act request served on the City requires such a search and must be transmitted to the City Clerk within that time.

5.15. Remote Network Access

Access to the City's network is available via a secure VPN or web remote access portal for employees and support personnel that need to work remotely. Employees desiring this capability may submit a written request, subject to Department Head, Human Resources, and IT approval. Installation of any unauthorized remote access software is strictly prohibited. The City's VPN is to be used only for official City business only. The VPN can be accessed only on City-owned and controlled computers; exceptions may be granted as needed for remote support from approved vendors. VPNs that are created for support from outside vendors will be enabled only for the time period that they are active and/or need to provide service. When they are finished with their task, the account will be deactivated until next use.

5.16. File Management

All documents, files, and electronic data should be electronically stored on the network file server in order to preserve the information via regular daily system backups performed by the Information Technology Division. Appropriate locations for file storage are the departmental directories on the (I:\) drive or the employee's individual directory on the Personal (P:\) drive.

Employees should not store any files on their local computer (c:\drive) or any other local drive on their desktop computers as these files will not be backed up and may be lost due to a system failure or corruption.

All original City documents and records are the property of the City and shall be maintained in accordance with federal, state, local laws, and City policies and procedures. Employees/agents shall ensure that City records will be retained in accordance with the City's records retention policy.

Employees should regularly review files they have created and placed on the shared drives to decide what can be deleted or purged from the system in accordance with the City's records retention policy.

Storage of City data on Mobile Devices, personally-owned devices such as smartphones, laptops, or home computers, or on unapproved Internet or "Cloud" based services, is prohibited.

Storage of copyrighted multimedia files (including music and videos) on City computers or servers is prohibited.

Any material found on City computers or servers that does not directly relate to the job duties of the employee and/or the employee's department may be deleted and the employee's supervisor and/or department manager notified.

5.17. Service Requests

Problems with computer equipment, software, or other related problems shall be reported to the IT staff immediately. Employees shall not attempt to resolve any unfamiliar problems without IT assistance. All service requests regarding hardware, software, or network problems should be directed to the Helpdesk at help@san-clemente.org. In order to serve the City efficiently, avoid contacting individual IT staff members directly.

5.18. Security Awareness and Education

The City takes protecting the organization, its intellectual property and any personal or confidential information extremely seriously. To help protect the City, training will be provided to all staff members who use a computer to perform their duties. The goal is to help individuals understand the risks in using today's technology and how to effectively defend against cyber threats, both at work and at home.

All personnel will be required to take annual training, usually in the form of on-line video training or onsite workshops. The City may also provide reinforcement training such as newsletters, webcasts and other means. In addition to training, the City's security awareness and education program will include unscheduled awareness assessments to assure compliance with the training. Any employee who fails to take required training, or who continually fails periodic assessments may be subject to disciplinary action as outlined in the City of San Clemente Personnel Rules.

Virus protection software is installed on each computer. Users shall not disable this software. Users will notify the IT staff of any virus detection messages they receive on their system. City Employees must report suspected information security incidents immediately to the Information Technology division. All suspected intrusions of the City Network by unauthorized employees or other individuals are to be reported to the Information Technology Division immediately.

Users should inform the appropriate Information Technology personnel when the user's software does not appear to be functioning correctly. If the user, or the user's manager or supervisor, suspects a computer virus infection, these steps should be taken immediately:

- Stop using the computer
- Do not try to save data.
- Turn off the computer.
- If possible, physically disconnect the computer from networks to which it is attached.
- Contact IT.

5.19. Enforcement and Violations

The City reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Violations of this policy will be reviewed on a case-by-case basis and may result in disciplinary action as outlined in the City of San Clemente Personnel Rules.

6. PROCEDURE:

6.1. This policy will be reviewed by the Information Technology Manager on an annual basis and may be updated as needed with City Manager approval.

6.2. Any violation of this policy may result in loss of computer access and disciplinary action, up to and including termination.

6.3. All City employees and individuals subject to the provisions of this policy will receive a copy of the policy and be required to sign an acknowledgment form. Individual signed forms will be retained in the employee personal file or other appropriate file in the Human Resources Division.

ACKNOWLEDGMENT OF RECEIPT AND UNDERSTANDING OF THE USE OF INFORMATION TECHNOLOGY POLICY

This will acknowledge that I have received my copy of the City of San Clemente Acceptable Use of Technology policy and that I have read the policy and understand my rights and obligations under the policy. Furthermore, I understand that I have no reasonable expectation of privacy with respect to my use of the City's technology related systems, electronic equipment, or other communication devices.

I understand that employees and authorized individuals must sign an acknowledgment that they fully understand the policy and will comply with the procedures set forth in the policy. My signature below signifies that I have read this policy and that I accept and will abide by all of its provisions.

PRINT FULL NAME _____

SIGNATURE _____

DATE SIGNED _____