COMPUTER USAGE AND SECURITY POLICY

PURPOSE: To establish the proper use of the City of Moreno Valley's computer systems. The procedures and principles represented in this policy apply to anyone accessing the City network, including all City Employees (see the definition below) who use City-provided computer equipment.

DEFINITIONS AND TERMS:

City Employee: Any person or entity compensated by the City or volunteering with the City. This includes, but is not limited to, full-time employees, part-time employees, temporary employees, elected officials, volunteers, commissioners, contract employees, partners, vendors, contractors, and other affiliates.

Computer: This term is used generically to refer to any technology used to work on City business. It includes, but is not limited to, desktops, laptops, tablets, servers, smart phones, personal digital assistants, radios, repeaters, cameras, and mobile devices.

File Server: A computer that is responsible for the central storage and management of data files and applications.

Private Directories: All employees are setup with a Private Directory designated as V:\ that can be accessed by that employee only.

Public Directories: All employees are set up with a Public Directory designated as W:\ that can be accessed by any employee in their work group.

Application Directories: All employees are set up with an Applications Directory designated as O:\. The employee will not be able to access any application that they do not have specific permission to access.

Other Directories: Employees should not attempt to gain access to a file or directory that does not pertain to their specific job function. Casual browsing of the network is not permitted.

I. INTRODUCTION

Computers and networks are an integral part of business at the City of Moreno Valley. The City has made a substantial investment in human and financial resources to create these systems. The enclosed policies and directives have been established in order to:

- Protect this investment;
- Safeguard the information contained within these systems;
- Reduce business and legal risk;
- Protect the good name of the City.

A. Authority

This policy has full support from the City Manager's Office. The Technology Services Division Manager administers this policy. This policy is effective for all City Employees and all Computers.

B. Contents

The topics covered in this document include:

- Statement of responsibilities
- The Internet
- E-mail
- Computer malware
- Access codes and passwords
- Computer use
- Copyrights and license agreements

C. Continuance

This policy is a living document and may be modified at any time by the Technology Services Division Manager, subject to final approval by the City Manager. Modifications will be communicated to employees in a reasonable time. Modifications do not invalidate an employee's signature and consent to the policy.

II. 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. Technology Services Responsibilities

The Technology Services Division must:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
- 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.
- Change vendor default passwords on all hardware and software before being placed on the network or used for City business.
- 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.

III. THE INTERNET

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. To establish proper use of the Internet, the procedures and principles presented in this policy apply to all City Employees.

A. Policy

Use of the Internet for personal gain or any other purpose which is illegal or against City policy or contrary to the City's best interest is prohibited. Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive and to protect the City's interests, the following guidelines have been established for using the Internet.

City Employees are not automatically given access to the Internet. An employee will need to have specific permission from their supervisor to have access to the Internet. A separate Internet Access Agreement form will need to be read and signed by the employee and his or her department head.

B. Establishing Accounts With Other On-Line Services

Employees who need to establish an account with an on-line service via the Internet must use a different password than their City password

C. Internet Access is a Privilege

Unauthorized use of the Internet will result in the loss of access for the user and, depending on the seriousness of the infraction, may result in disciplinary action as deemed appropriate.

D. Acceptable Use

Employees using the Internet are representing the City. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Viewing training videos that directly relate to your job.
- Attending a job related webinar or meeting.
- Using Web browsers to obtain business information from commercial Web sites.
- Accessing databases for information as needed.

E. Personal use

Incidental and occasional personal use of the Internet as covered by this policy may be permitted at the discretion of the Division Manager and/or Department Director. 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.

F. Unacceptable Use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the City, or nonproductive. Examples of unacceptable use include but are not limited to:

- Conducting a personal business using City resources.
- Transmitting any content that is offensive, pornographic, harassing, or fraudulent.
- Accessing e-mail accounts from the Internet such as Gmail, Hotmail, Yahoo mail and any other Internet related mail accounts. Accessing e-mail in this manner bypasses the City's e-mail antivirus scanning software and introduces a risk of malware infection to the City network.
- Playing games or gambling is not permissible anytime whether over the Internet or on a stand-alone computer.
- Downloading or receiving via e-mail non-business related music files or video files.
- Streaming Radio/music/video: An extensive amount of bandwidth is used to access these sites and is not permitted unless being conducted for official City business.
- Downloading, receiving via e-mail or importing into the City via removable media, any type of screen saver, desktop themes, animated characters, etc. Some of the screen savers and desktop themes are not free, and if not purchased by the City, violates the software copyright law. Also some of these programs can conflict with other programs existing on the computer.
- File downloads from the Internet are <u>not</u> permitted unless specifically authorized by the Network Administrator.
- Do not allow anyone access to your PC via the Internet. WebX applications enable a vendor to take control of your PC through the Internet. Typically, you access a web site, and then join a meeting with the vendor. At that time the vendor can take full control of your PC. This type of access is not permitted without prior consent from the Network Administrator.

G. Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the City and/or legal action by the copyright owner.

H. Monitoring

Technology Services monitors Internet access. Accessing Internet websites that are deemed unacceptable under this policy will result in disciplinary action.

IV. E-MAIL

E-mail is considered a communication of the City and, once retained pursuant to subsection C below, will be held to the same standard as formal letters or memorandum. Technology Services has the ability and authority to monitor employee e-mail activity as it applies to the normal course of business when there are reasonable grounds to do so per the request of proper management/supervisory staff. Users should not consider Internet e-mail to be either private or secure and should have no expectation of privacy.

A. Internet E-Mail

Only employees with a valid network login and e-mail account can send/receive e-mail via the Internet.

B. Technology Services Responsibilities

Technology Services shall perform an electronic backup of the City's e-mail system each evening. The backup is a "snap shot" of the data contained on the e-mail server at the end of the business day. The backup is not a copy of all activity that occurred within the e-mail server during the day.

Technology Services shall maintain the electronic backups of the City's e-mail system for a period not longer than two (2) weeks. The backups of e-mail are not to be considered a backup for public records purposes. The purpose of backups is to provide a means of complete server recovery in the case of a system failure.

Technology Services has established an e-mail management system that will automatically remove e-mail in the Deleted Items and Sent Items folders (and any subfolders), that are 30 days old, e-mail in the Inbox (and any subfolders) older than 90 days, and e-mail in user created folders in the Mailbox older than 90 days.

C. City Employee Responsibility for E-Mail Records Retention

The purpose of this policy for the use of electronic communications is to provide guidance to City Employees regarding the proper and authorized use of the City's e-mail system in accordance with the requirements of the Public Records Act as well as the requirements of the City's Records Retention Schedule and the laws and regulations governing it, and other laws and regulations that apply to public agency information. E-mails may be subject to public disclosure under the Public Records Act, cooperation with law enforcement, or litigation.

If any employee has any questions regarding the implementation of this Policy, contact either: the City Attorney's office (for legal questions, such as an interpretation under the Public Records Act); the City Clerk's office (regarding the Records Retention Schedule); or Technology Services (regarding any technical issues related to the use of the e-mail system).

Do not forward a confidential e-mail to any unauthorized recipient. E-mail which contains confidential attorney-client information or attorney work-product may not be disclosed to non-City personnel except by the City Attorney's Office, unless so authorized by the City Manager or his or her designee, or as required under law.

The e-mail system shall be used for transmission, communication, and organization of City business that is transitory. The e-mail system shall not be used for storage of items subject to the City's Records Retention Schedule. The e-mail system is provided by the City to employees as a convenient and efficient method of rapidly communicating transitory information in an electronic format. The e-mail system is specifically intended and designed to be a tool for transmission of information, and not a tool for permanent storage. Since information on the e-mail system is automatically purged, the City shall consider every e-mail to be a preliminary draft, note, or memoranda and not retained in the ordinary course of business.

For each e-mail sent or received, employees shall determine whether or not there is information on

the e-mail which is required to be retained for the discharge of the employee's official duties for the City. This determination shall be made using the same criteria which is applied to information sent or received by the employee using any other means of communication. If an e-mail contains information which is "required to be retained", the employee shall: (1) transfer the required information from the e-mail to an appropriate public record storage system (such as printing the e-mail) before it is deleted or purged from the e-mail system, and (2) maintain the public record in accordance with the City's Records Retention Schedule. E-mail messages should be filed with program records where they are subject to the same retention schedule as the records with which they are filed.

D. City Employee Responsibility

- Use e-mail for business contacts.
- Compose e-mail in a professional manner.
- Report changes to information included in the automatically generated e-mail signature in a timely manner.
- Any employee receiving attachments via Internet e-mail shall treat those attachments as they would any unknown file by scanning it with the antivirus software BEFORE opening it. In addition to malware transmitted via e-mail, there is malware that is spread by being embedded in Word, Excel, photo, and PDF files.
    - To scan a file or folder/directory before opening it: Save the file to your PC; Open Windows Explorer; Right-Click on the item; and Choose the option to "Scan with ESET Endpoint Antivirus" or whatever antivirus software is installed.
    - The VirusTotal website is also useful when determining if a file is safe to open or if a link is safe to follow. See https://www.virustotal.com.
- Check incoming e-mail several times per day to ensure a timely response in answering unopened mail messages.
- Establish a method of having their e-mail monitored while they are away from the office on planned and unplanned absences.
- The e-mail system is not intended to be an archival system. Any e-mail that needs to be saved should be printed and filed accordingly.
- Clean out Inboxes, Sent Items and Deleted Items folders on a regular basis (weekly). Once the Deleted Items folder has been emptied, there is a seven (7) day period where the e-mail can still be recovered. After seven days, the e-mail cannot be retrieved by the user. If e-mail needs to be restored complete a help desk ticket and Technology Services may restore the e-mail.

E. Unacceptable Use

- Opening an e-mail attachment you are not expecting to receive. The most destructive malware to date are e-mail malware hidden as an attachment and malware imported on a flash drive.
- Sending or receiving any sexually oriented messages or images.
- Sending e-mail containing offensive or harassing statements, including comments based on race, color, gender, age, physical or mental disability, religion, national origin, pregnancy, physical attributes, sexual preference, political beliefs, or any other protected status.
- Taking actions that cause interference to the network or to the work of others.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Subscribing to more than five (5) Internet e-mail list servers.
- Sending messages in an attempt to "flood" receiver's e-mail box.
- Sending copies of documents in violation of copyright laws.
- Adding background images to an e-mail.
- Do not use your City e-mail address for personal use, such as receiving notifications for sales ads or mortgage rates. Giving out your City e-mail address for personal use could increase

the amount of SPAM the City receives. Use your City e-mail address for official business only.

- Sending e-mails to more than 100 recipients at a time or repeatedly sending a smaller number of e-mails that accumulate to 100. Behavior such as this makes the City appear to be sending SPAM and will cause the City to be blacklisted. Removing the City from an e-mail blacklist is very time consuming and results in lost productivity for all employees.

F. Use of Address Book

- Public Groups: Selection of the Public Groups feature will enable the employee to access distribution lists specifically created for use citywide. Technology Services is responsible for the creation of Public Groups.
- Personal Group: Selection of personal group feature will enable the employee to create, edit or delete his or her own Personal Groups.
- Resources: Selection of the Resources feature will allow employees to request available Resources such as conference rooms, overhead projectors and other types of equipment.
- External Address: Selection of this feature is used for external addresses such as the Police Department external addresses are a citywide feature. If multiple employees have a need for an external address, Technology Services can place it in the External Address list.

G. Monitoring

Because all computers, software and telecommunication systems remain the property of the City and are for official use only, all records, files, transmissions, passwords and other products or contents of these systems are not confidential and may be reviewed at any time by City management or its designee(s). Therefore, employees shall have no expectation of privacy in any documents or other materials they write, receive, store or send in the use of these systems.

All messages created, sent, or retrieved over the Internet are the property of the City and may be regarded as public information. The City of Moreno Valley reserves the right to access the contents of any messages sent over its facilities if the City believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. Therefore, do not put anything into your e-mail messages that you would not want to see on the front page of a newspaper or be required to explain in a court of law.

H. SPAM (Unsolicited e-mail)

Unsolicited e-mail is known as SPAM. Technology Services has a system in place to block the majority of SPAM. Approximately 70% of all e-mail entering the City network is SPAM. People that create SPAM e-mail constantly devise ways to bypass anti-SPAM systems. Technology Services makes every effort to block SPAM, but occasionally SPAM e-mail will slip past the system. Notify Technology Services if you consistently receive offensive SPAM; otherwise, just delete any SPAM you may receive.

V. COMPUTER MALWARE

Malware is short for malicious software. Malware is any kind of unwanted software that is installed without your consent. Viruses, worms and Trojan horses are examples of malicious software that are often grouped together and referred to as malware. Therefore, malware can cause the destruction of City resources.

A. Background

It is important to know that:

- Computer malware is much easier to prevent than to cure.

- Defenses against computer malware include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining antivirus scanning software.
- The most destructive malware to date has been initiated through e-mail as an attachment or imported through a flash drive.

B. Technology Services Responsibilities

Technology Services shall:

- Install and maintain appropriate antivirus software on all Computers.
- Respond to all malware attacks, any malware detected, and document each incident.
- Monitor network activity/traffic for attempts at gaining unauthorized access.
- Keep anti-virus software definitions updated hourly.

C. Employee Responsibilities

These directives apply to all City Employees:

- Employees shall not knowingly introduce malware into Computers.
- Employees shall not load CDs, or flash drives of unknown origin or content.
- Incoming, CDs, flash drives and external hard drives shall be scanned for malware before they are read.
    - To scan a file or folder/directory or entire USB device before opening it: When inserting a USB device a windows will pop up giving you several options; Click on the option to "Open folder to view files"; Right-Click on the item; and Choose the option to "Scan with ESET Endpoint Antivirus" or whatever antivirus software is installed.
- Any employee who suspects that his/her workstation has been infected by malware shall IMMEDIATELY POWER OFF the workstation and call the Network Administrator.
- If equipment that was not issued by the City is to be connected to the network then it must be shown that the equipment has current anti-malware software installed and active. The Network Administrator will make this determination; contact Technology Services in order to have them evaluate the equipment.

VI. ACCESS CODES AND PASSWORDS

The confidentiality and integrity of data stored on City Computers must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties. An automated password policy is set to require employees to change their domain password every 90 days.

A. Technology Services Responsibilities

The Technology Services Division Manager shall be responsible for the administration of access controls to all City Computers. The Technology Services Division Manager will maintain a list of administrative access codes and passwords and keep this list in a secure area. The Network Administrator will change the domain administrator password and all other system level passwords every 90 days.

B. Employee Responsibilities

Each employee:

- Shall be responsible for all computer transactions made with his/her User ID and password.
- Shall not disclose passwords to others. A password must be changed immediately if it is suspected that it has become known to others. Passwords should not be recorded where they may be easily obtained.
- Should use passwords that include a combination of letters, numbers or characters. Passwords should be at least **8** characters long, cannot be found in the dictionary, will not be easily guessed by others, and contain characters from 3 of the following 4 groups: upper-case, lower-case, special, and numbers. An example of a **secure** password is: **Tx*cE2mm**.

- Should log out when leaving a workstation for an extended period.
- Ensure that accessing City resources from a remote location such as home or a hotel will not let any unauthorized person access City e-mail, data or resources. Unauthorized access is a breach of this policy and disciplinary actions will be taken.
- City employees who are allowed to access the City network are given a network login account. Employees are **not allowed** to let anyone use their City login (except Technology Services staff for in-person troubleshooting purposes).
- Consultants are not allowed to access the City network unless they have permission from the Network Administrator.

C. Supervisor's Responsibility

Managers and supervisors should promptly notify Technology Services (via the Helpdesk application) whenever an employee hires-on, leaves, or transfers within the City so that his/her access can be added, revoked, or modified accordingly. Involuntary terminations must be reported concurrent with the termination.

D. Human Resources Responsibility

Human Resources will notify Technology Services weekly of known employee hires, transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

VII. COMPUTER USE

It is City policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

A. Employee Responsibilities

The directives below apply to all City Employees:

- Any attempt to interfere with, prevent, obstruct, or dissuade an employee in their efforts to report a suspected information security problem or violation is strictly prohibited and cause for disciplinary action, up to and including dismissal and possible prosecution to the fullest extent of the law. Any form of retaliation against an individual reporting or investigating an information security problem or violations is prohibited.
- CDs, flash drives and external hard drives should be stored out of sight when not in use. Highly sensitive or confidential data must be locked in a cabinet or desk drawer.
- CDs, flash drives and external hard drives should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
- Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). A surge suppressor should protect other computer equipment.
- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
- Since the Network Administrator is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by Technology Services.
- Employees shall not take City-owned computer equipment (monitors, desktop computers, printers) out of City buildings without the informed consent of their Division Manager. Informed consent means that the Division Manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
- Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.
- All data should be stored on the file server. Each employee will have his or her own private folder to store data on the server. Data should not be stored on the local computer (C: and/or D: and/or E: drives). Technology Services is not responsible for any data stored on the local

computer. Data stored on the local computer cannot be backed up and is not secure.

- Network equipment such as routers, modems and switches are not to be installed/used without the permission of the Network Administrator. Employees are not allowed to "browse" the network and open/read files that do not relate to their specific duties.
- All electronic documents and electronic forms to be used outside of a department must be reviewed by the Technology Services Division during development and prior to distribution to attempt to standardize and automate the forms.
- Inter-department or intra-department databases intended to be used by more than one person requires a consultation with the database administrator during development and prior to distribution.
- Requests for Technology Services should be processed through the Helpdesk application.
- Users will either log off or lock their workstations when they will be away from the computer for any length of time. Users can also set their screen saver to use the "password protected option" and set the wait time for no longer than 10 minutes.
- Personal photo, music, video, or other non-business related files are not to be stored on City servers or workstations.
- Wireless Access Points are not to be connected to the City of Moreno Valley network under any circumstances. If a Wireless Access Point is discovered it will be disconnected immediately.
- City staff accessing the Department of Motor Vehicles (DMV) network must not copy or store any DMV data to another database system.
- City staff accessing the DMV network must not copy or store DMV data beyond its intended business purpose.
- City staff accessing the DMV network must not copy or store DMV data on any computer or server.

B. Personal Cell phone/Smartphone

- Personally-owned cell phones/smartphones are allowed to connect to the City e-mail system but the City is not obligated to assist or make the connection work. Submit a Helpdesk ticket to Technology Services to obtain the information necessary to connect your cell phone/smartphone to the e-mail server.
- Personally-owned cell phones/smartphones are not allowed to connect to a City workstation; this includes but is not limited to synchronization software, Universal Serial Bus (USB), FireWire or other hardware or cabling.
- If and when malware become a problem with cell phones/smartphones and antivirus software is available, the City, at its sole discretion, may require such software before cell phones/smartphones are allowed to connect to City systems. The purchase of such software will be at the owner's expense.

VIII. COPYRIGHTS AND LICENSE AGREEMENTS

The City of Moreno Valley and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose the City and the responsible employee(s) to civil and/or criminal penalties.

A. Scope

This directive applies to all software that is owned by, or licensed to, the City of Moreno Valley, or developed using City of Moreno Valley resources.

B. Installation and Support of City of Moreno Valley Software

The City of Moreno Valley Technology Services Division is exclusively responsible for installing and supporting all software on City Computers.

The City of Moreno Valley Technology Services Division relies on installation and support to provide software and hardware in good operating condition to City employees so that they can best accomplish their tasks.

C. Technology Services Responsibilities

The Enterprise Systems Administrator will:

- Maintain records of software licenses owned by City of Moreno Valley.
- Periodically (at least annually) scan company computers to verify that only authorized software is installed.

D. Employee Responsibilities

Employees shall not:

- Bring software from home and use it on their computer.
- Install or play games on their computer.
- Install software unless authorized by Technology Services. Only software that is licensed to or owned by City of Moreno Valley is to be installed on City Computers.
- Copy software unless authorized by Technology Services.
- Download software unless authorized by Technology Services.

Employees shall:

Upon termination of employment, uninstall any Microsoft "Home Use Program" (HUP) software that may have been purchased through the HUP and return the installation disks to the Human Resources Department along with any other City property.

E. Violations

Violations may result in disciplinary action in accordance with City policy. Failure to observe these guidelines may result in disciplinary action by the City depending upon the type and severity of the violation, whether it causes any liability or loss to the City, and/or the presence of any repeated violation(s).

F. Civil Penalties

Violations of copyright law expose the City and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

G. Criminal Penalties

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b))," expose the company and the employee(s) responsible to the following criminal penalties:

- Fines up to $250,000 for each illegal copy
- Jail terms of up to five years

ATTACHMENT A

Acknowledgment of Computer Usage and Security Policy

This form is used to acknowledge receipt of, and compliance with, the City of Moreno Valley Computer Usage and Security Policy.

Procedure:
Complete the following steps:

- Read the Computer Usage and Security Policy.
- Sign and date in the spaces provided below.
- Return this page only to the Technology Services Division Administrative Assistant.

Signature:
By signing below, I agree to the following terms:

1. I have received and read a copy of the "Computer Usage and Security Policy" and understand the same.
2. I agree that I will not use City resources to transmit images and/or text that is derogatory and/or harassing based on race, color, gender, age, physical or mental disability, religion, national origin, pregnancy, physical attributes, sexual preference, political beliefs, or any other protected status.
3. I understand and agree that any computers, software, and storage media provided to me by the City of Moreno Valley contains proprietary and confidential information about the City of Moreno Valley and its customers or its vendors, and that this is, and remains, the property of the City of Moreno Valley at all times.
4. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at the City of Moreno Valley), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software.
5. I understand that the security of the City's network is of vital importance. I will keep my password confidential. I will not allow unauthorized persons to access the City's internal networks. I will promptly report any use of my account by others to the Technology Services (TS) Division. I understand that TS may immediately terminate my remote access in the event of a security breach.
6. I agree that if I leave the City of Moreno Valley for any reason, I shall immediately return to the City the original and copies of any and all software, computer materials, or computer equipment that I may have received from the City that is either in my possession or otherwise directly or indirectly under my control.

_____
Employee Name (please print)

_____
Employee Signature

_____
Date

_____
Department

INTERNET ACCESS RELEASE

By signing this release, the undersigned employee agrees that he/she has read and understands Technology Services Policy #7.10 and will abide by the policy. Specifically, the undersigned acknowledges that: **(1) Internet access will be for official City Business, (2) Exchanges that occur in the course of conducting City business on the Internet will be considered a communication of the City and held to the same standards as formal letters, and (3) Technology Services has the authority and ability to monitor and restrict the user's Internet activity.** *Any personal use of the Internet shall only be done with the supervisor's knowledge and permission and shall not interfere with the City's business. In addition, the undersigned employee agrees to the following:*

City of Moreno Valley Employee Internet Users WILL:

⇒ Take all reasonable precautions against importing computer malware. This includes scanning files obtained through the Internet utilizing antivirus software *BEFORE* the file is accessed in any way.

⇒ Use common sense, erring on the side of caution, at all times.

City of Moreno Valley Employees **WILL NOT**:

⇒ Operate a business through the City's Internet link.

⇒ Send or receive sexually-oriented messages or images.

⇒ Subscribe to any non-work related list servers.

⇒ Send mail or other communications, files or programs containing offensive or harassing statements, including comments based on race, color, gender, age, physical or mental disability, religion, national origin, pregnancy, physical attributes, sexual preference, political beliefs, or any other protected status.

⇒ Take actions that cause interference to the network or to the work of others.

⇒ Participate in gambling or other Internet-based games.

⇒ Copy, download or distribute any unauthorized copyrighted materials including but not limited to messages, e-mail, text files, program files, image files, database files, sound files and music files.

Employee Name (please print)	Division Manager Approval -- OR --
Employee Signature	Department Head Approval
Date	