Number: 03.002.00

City of Riverside
Administrative Manual

Effective Date:	07/2003
Latest Revision Date:	05/2018
Next Review Date:	07/2020
Policy Owner(s):	Innovation and Technology Department

Approved:

Department

Al Zelinka
City Manager

SUBJECT:

Technology Use and Security Policy (TUSP)

Purpose:

This Technology Use and Security Policy establishes guidelines for the proper use and security of City of Riverside (City) Technical Resources and non-City owned Technical Resources when used to conduct City business or communicate with City employees or representatives.

Definitions

Technical Resources include hardware, software, services, computers, computing facilities, peripherals, network components, mobile devices, tablets, applications, databases, websites, materials, accounts, subscriptions, intranet, voice-mail, digital cameras, and other technology and infrastructure provided by, paid for, or used in conjunction with the City, excluding the administration of the California Law Enforcement Telecommunications System (CLETS), Criminal Justice Information Services (CJIS), and Supervisory Control and Data Acquisition (SCADA) systems, which shall still adhere to applicable regulations and best practice principles.

City Internal Technical Resources refer to non-public facing technology assets, data or applications hosted within City facilities, offsite or hosted through third party providers.

City Information includes without limitation, e-mail, accounts, subscriptions, data files, instant messages, pictures, images, video clips, audio files and voice-mail that an employee, vendor, contractor or their employees create, stores, transmits, retrieves or receives using City Technical Resources.

Users include all City employees, managers, vendors (contractors, consultants, subcontractors), volunteers, elected officials, and other personnel or persons who use or access City Technical Resources and City Information.

CIO refers to Chief Innovation Officer or designee.

Scope

This policy applies to all Technical Resources designated for City business use. This policy also applies to any related services provided or paid for by the City, such as wired or wireless Internet and network

access, city-owned or stipend phones, computers, voice-mail, instant messaging, and e-mail, whether or not these services are on City premises, externally hosted, accessed remotely using virtual private network (VPN) or shared electronically. Users shall use these resources only in accordance with this policy. Any use of mobile devices for City business must comply with the Mobile Communications Device Policy, see *Administrative Manual Policy No. 03.007.00.*

All City employees, managers, contractors, vendors, volunteers, and other personnel or persons who use or access internal City Technical Resources and City Information must comply with the requirements of this policy.

Compliance

All employees or vendors using City Technical Resources are responsible for the content of all files, text, audio, information, data, and images that he or she saves, transmits, creates, accesses, views, or sends using City Technical Resources.

All users are responsible for complying with City security policies, standards, processes, and procedures. Innovation and Technology staff must build, configure, operate, and maintain networks and systems in accordance with these policies, standards, processes, and procedures. Anyone becoming aware of violations of this policy will immediately bring this to the attention of the appropriate department authority and the CIO.

Outsourced services, processing and storage facilities (such as service bureaus, vendors, partnerships, and alliances) and their subcontractors must accept, enforce, and agree to City's Technical Use and Security policy and regular compliance audits. Acceptance of the terms of this policy is mandatory for all vendors prior to gaining access to store, transmit, process, or access City Technical Resources.

Acceptable Uses of Technical Resources

Users must use the City Internet and e-mail systems in accordance with the Technology Use and Security Policy. The City may use tools to block or limit access to Internet or Technical Resources that lack a City business related role. The ability to access an Internet site, application, network or service from a City system does not constitute authorization or endorsement to use that Internet site, application or network. Users shall not allow family members or non-authorized Users to use City computers, Internet, intranet, applications, remote access systems, or other City Technical Resources.

- Technical Resources are provided for City business and must be limited to such use, except as otherwise provided in this policy.
- An employee may access only the files and information that he or she is authorized to access.
- Citywide e-mail messages will be limited to work-related announcements or emergencies affecting, or of interest to, the majority of City users. Authorized Users may request e-mail messages to be sent as broadcast e-mail messages by sending them to the City Manager's Office for approval and distribution. City management will determine if the e-mail qualifies for Citywide distribution. City management may deem the e-mail messages more appropriate for smaller distribution. For additional information, please see *Administrative Manual Policy No. 01.014.00, Use of Mass Internal E-Mails.*
- Employees who wish to express personal opinions or perform non-work-related tasks on the Internet or via mobile devices are encouraged to obtain a personal account with a commercial Internet service provider outside of City facilities.
- During breaks, employees may use their own electronic devices on the City's free public Wi-Fi for personal use.
- Users may use the Technical Resources for occasional minimal non-work purposes during mealtimes, breaks, or outside of work hours with permission from their Department Head or

designee and provided that all other elements of this policy are followed. E-mail messages of a non-work nature must be minimized.

- Authorized representatives of City departments who wish to utilize social media to enhance further communications with organizations in support of City goals and objectives must seek approval from their Department Head and submit the request to the City's Communications Office before creating any City-hosted social media site, and must follow the City's Social Media Policy - *Administrative Manual Policy No. 03.012.00 - Guidelines for Social Media Usage.*

Unacceptable Uses of Technical Resources

- Users may not use the Technical Resources for non-work purposes including but not limited to accessing dating sites, playing games, downloading files, streaming videos, music, accessing personal E-mail or other unauthorized non-City related business or activity as determined by their Department Head or supervisor.
- Technical Resources are not to be used in a manner that may interfere with or degrade City business operations as determined by the Innovation and Technology Department.
- Users are prohibited from using another user's password.
- Users are prohibited from using generic shared accounts except by express permission of the CIO.
- Users are prohibited from sending an e-mail or other communications that masks the sender's identity or indicates that the e-mail was sent by someone else.
- City users are prohibited from using non City authorized e-mail systems for City business.
- Use of the Internet/the web, intranet, electronic bulletin board or other Technical Resources to harass or discriminate is unlawful and strictly prohibited by the City.
- Users and others are prohibited from sending, saving, creating, forwarding, accessing or viewing material using Technical Resources if said material could be reasonably considered offensive, including but not limited to pornography, sexual, sexist, or racist comments, jokes, slurs, or images, on the basis of race, color, creed, sex, age, national origin, ancestry, physical or mental disability, veteran status, sexual orientation, or other category protected by federal, state, or local laws. All Users using Technical Resources, including publicly owned computers located at any City Facilities including Libraries and Recreation Centers, are strictly prohibited from accessing or viewing pornography, nudity, obscene material, and dating sites.
- Uses that interfere with the proper functioning of the City's Technical Resources are prohibited. Such inappropriate uses include the creation or distribution of viruses into computer systems, e-mail spam, chain letters, keyboard loggers, malicious destruction of another's files, use of software tools that attack, disables or circumvents security City or external Techical Resources, and other violations of security standards.
- Use of City Technical Resources for personal or financial gain.
- Using the name of the City, City affiliate or City subdivision in personal messages, or otherwise making statements in messages that might be mistaken for the position of the City, City affiliate or City subdivision. Users may not post content or conduct any activity that fails to conform to any and all applicable state and federal laws.
- Installing or connecting any unauthorized device, including personally-owned flash removable media or cell phones to a City owned Technical Resource or the City network. Personally owned cell phones may be charged using electric outlets.
- Soliciting for any non-City business or activities using City resources.
- Use of Technical Resources in a manner that interferes with the employee's productivity, the productivity of any other employee, or the operation of City Technical Resources.
- Use of City's Technical Resources to participate in online tournaments or auctions for non-work related matters.
- Violation of any federal, state or local law or regulation, including without limitation, defamation of person or trade, securities laws, gambling, threats to harm any person, property or the environment, intentional transmission of a computer virus, harmful computer program, trade secrets, and violation of trademark, copyright, or other intellectual property law.

City Monitoring

- By using the City's Technical Resources, users acknowledge they have no right or expectation of privacy in the use of City Technical Resources, and the City reserves the right to monitor, review, and log such use without prior notification.
- The City may use software and other means to inspect files, or monitor an individual's use of any City Technical Resources, with or without notice.
- The City uses software and other means to attempt to block or restrict access to websites containing material that violates this policy. An employee attempting to intentionally access blocked websites is in violation of this policy.
- Even when files, data, e-mail messages, instant messages, images, or voice messages are deleted, or the Internet or web sessions are terminated, it may be still possible to recreate them.

Identification, Authentication, and Authorization

Access to all internal City Technical Resouces requires robust, continuous and reliable authentication. Each Department Head or designee will approve all new accounts through the City's Move Add Change (MAC) form that can be accessed via the City's intranet. New accounts will be set up in accordance with this policy and any applicable department requirements. Each user must be identified and authenticated using a standard, unique, personally assigned login. Standard user accounts will be granted limited authorization to perform daily tasks. Innovation and Technology administrators will be assigned an additional unique, personally assigned login. The use of administrative logins shall be limited to authorized systems, network and applications administrative tasks. Users are strictly prohibited from sharing login credentials. Upon separation of an employee, the Department Head or designee will submit a MAC form to remove the employee's access to the City's technology systems. Accounts shall be disabled for 90 days prior to deletion unless longer retention is required by a regulating agency.

Passwords Management

All passwords must be strong and well-guarded. Users are responsible for choosing passwords that are highly secure. The use of passphrases instead of passwords is highly recommended. Users shall never divulge their passwords to others, even their supervisors, fellow employees, or IT staff. Improper or unauthorized disclosure of login information, passwords, or other confidential information is subject to discipline up to and including termination.

- All passwords should be treated as sensitive, confidential, and protected information.
- Password sharing is strictly prohibited. Exceptions may be granted by the CIO upon request.
- If a user discloses login information, passwords, or other confidential information they must immediately change any passwords and report it to their supervisor and the Help Desk at extension 5508 or HelpDesk@riversideca.gov.Writing down passwords is not an acceptable practice, however, if passwords must be recorded, the information shall be stored only using an encrypted password manager and be accessible only by the owner.
- Storing passwords on user endpoints via electronic file or programmable function keys, scripts, macros, or automated login sequences including browser, device, or application automatic login is strictly prohibited.
- Storing user passwords in applications, databases, cloud providers, or mobile devices in plain text or using non-City approved encryption is strictly prohibited excluding embedded mobile email clients using Active Sync and Mobile Outlook. The use of default logins is strictly prohibited. Default hardware, software, vendor credentials, or application accounts must be changed to a unique password before being allowed on the network.User network login accounts will be disabled after three consecutive failed login attempts. Passwords will be automatically re-enabled after 30 minutes or can be reset by the Helpdesk, using a multi-factor identitiy verification process.

- Test, development, and training systems/environment should not store or use production systems administrative or user passwords.

The following is a list of general rules that users should follow to create strong passwords:

- Must be composed of a capital letters, lower case letters, numbers, and special characters
- Must be at least twelve characters in length
- Must be changed at least every 90 days
- Must never be the same as the user's login ID
- Must not contain the user's phone number or Social Security Number
- Must not be common words or phrases
- Must not be a name such as family member or pet
- Must be changed on first login
- Must not be changed more frequently than once a day
- Must not be reused within the last ten password changes
- Must not be posted physically on the user's work area or stored in plain text anywhere
- Must not to be reused on any non-City managed IT system, vendor, websites or device

Unattended Computers

Users will not leave confidential information present on screens if the workstation is unattended or while within public view. If a workstation will be unattended users must either log off or lock the system when they are away from the computer. Prior to departing any unsecured office areas or facilities where laptops or tablets are used, users must secure the device with a locking device/cable or remove them from the docking station and network (if applicable) and lock them in desks, containers or offices. IT will deploy an automatic screen saver application, requiring network password login after ten minutes of non-use. Exceptions may be granted by the CIO upon request.

Software Management

Any software installation, upgrade, or update runs the risk of introducing viruses, damaging the configuration of the computer, interfering with other IT systems or violating software-licensing agreements. The City must reduce the risk of introducing malicious code into the City network. As such, any software installation, upgrade, or update must be made in conjunction with the Innovation and Technology Department.

Outdated software can be riddled with vulnerabilities and poses significant threat to the City. All software, applications, and devices must be updated with the latest security patches to be allowed to function on the City's network. Exceptions may be granted by the CIO upon request.

Viruses, Malware, and Spyware Prevention

Spear-Phishing e-mail attacks are the source of the vast majority of breaches. Attackers attempt to entice unsuspecting users to open a malicious attachment or to click on a link exploiting the user's workstation granting them access to their workstation and potentially the entire network. Innovation and Technology shall deploy and keep current antivirus software updated on all City-owned and managed Technical Resources. However, because antivirus is signature-based, new viruses that have not been examined by the antivirus vendor can evade detection and infect City infrastructure. Users must notify the helpdesk if they clicked on an attachment or link that may have caused a malware, spyware, or virus infection or may have granted unauthorized access.

Software Downloads

To reduce the risk, all software downloads from the internet shall be blocked. Exceptions may be granted by the CIO upon request. Computers will be configured by the Innovation and Technology department staff to inhibit the downloading of unlicensed or unauthorized software.

Removable Media and File Sharing

All external removable media and non-City owned electronic devices should be treated as untrusted devices and should not be connected to the City's network. Internal and external file transfer, sharing and synchronization is only authorized through the City's secure file sharing platform. The use of non-City owned removable media, unauthorized third party file transfer software, and unauthorized sharing and synchronization services is prohibited without express permission of the CIO.

Software Licensing and Inventory

Software purchases must meet current City standards and conform to City procurement policies. Any exceptions requires express permission of the CIO. All software, including but not limited to, purchases or subscriptions, plugins, video or audio playback tools, mobile applications ("apps"), software as a service "SaaS" purchases, integration, and updates shall be installed and managed by authorized Innovation and Technology staff. Software must be licensed adaquately under the terms of the software developer's licensing agreement. Employees shall use software only in compliance with license agreements. Software will be installed only from approved sources. City departments will maintain an inventory of software applications used by their department and submit that inventory to the CIO.

City Access to Information

- City Management may retrieve, review, monitor, copy, or listen to any Technical Resources information when doing so serves the legitimate business interests and obligations of the City.
- City Information may be disclosed to law enforcement or other authorized third parties without an employee's prior consent or the consent of the sender or receiver of such information.

Remote Access

- The uploading of data to unauthorized third party remote file sharing, synchronization, or storage is strictly prohibited.
- Remote access to City internal technology assets, on-premise or in the cloud, is limited to methods approved by the CIO. A signed Technology Use and Security Policy (reference Appendix A) and Remote Access Agreement must be completed by the requester, and approved by the CIO or the Information Security Officer, before access will be authorized (reference Appendix C.)
- All remote network access requires the use of the City's dual-factor authentication system.
- Vendors will be granted remote escorted access through screen sharing software only as required. Unescorted access will be granted on an exception basis via express permission of the CIO.
- Upon implementation of technologies such as Virtual Desktop Infrastructure "VDI" or other VPN-less remote access, the City will not allow direct IP communication between untrusted remote devices and internal City IT infrastructure.
- Site to Site VPNs will only be granted as an exception subject to restrictions and audits by the City's security team and by express permission of the CIO due to the risk they introduce to the City through their connection.

- All systems hosting, processing, or directly communicating with internal City technology infrastructure will be subject to security, electronic discovery, and vulnerability audits.
- Information regarding City systems, such as server names, login information, IP addresses, VPN server IP addresses, or the data contained within are considered confidential. This information must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or made available to unauthorized third parties without express permission of the CIO.
- Vendors, partners, or contractors with physical, logical, or remote access to City Technical Resources or the data contained within may be required to obtain cyber-breach liability insurance or general liability insurance that covers cyber breaches naming the City of Riverside as an additional insured party. The City may hold a vendor liable in the event the source of a breach is traced to their employees, network, software, or hardware.
- Non-exempt users are prohibited from accessing Technical Resources, including City e-mail, via the Internet, or through other means outside regular work hours including during any paid or unpaid leave, without written authorization from their management. Failure to comply may lead to discipline. "Non-exempt" means an employee may be entitled to payment of overtime under certain conditions pursuant to the Fair Labor Standards Act.
- Exempt employees may access authorized Technical Resources, including City e-mail, remotely as necessary for the effective operation of City business except as indicated below. "Exempt" means an employee that is exempt from certain wage and hour requirements due to their duties and pay.
- Exempt employees are prohibited from accessing Technical Resources, including City email, via the Internet, or through other means while on paid or unpaid leave including but not limited to sick, Family and Medical Leave Act (FMLA), worker's compensation, military, and personal leave.

Database and System Access

Designated IT staff will be responsible for maintaining the data integrity, host environment, and users' access rights. Exceptions may be granted by the CIO upon request.

Physical Protection

Computer resources and physical information including, but not limited to, servers, storage, desktops, laptops, tablets, smartphones, network equipment, firewalls, sensitive paper and electronic records, backup tapes, and telephone equipment must have appropriate physical protections in place.

Classifying, Storing, and Handling Sensitive Information

Users must label, classify, handle, and protect City of Riverside paper or electronic sensitive/proprietary material according to the distribution and authorization levels specified for those documents to protect information integrity.

- All Users must safeguard the City's confidential information including business and financial information, as well as the confidential information of officials, officers, employees, affiliates, suppliers, vendors, residents, customers, and others. Disclosure of the confidential information is prohibited. Confidential information includes, but is not limited to, personally identifiable information (PII) such as Social Security Numbers, driver's license information, date of birth, health information, etc.
- If an employee needs to electronically transmit confidential data to an outside party, the employee must obtain his or her supervisor's approval. When the transmission is authorized, the data must

be protected using City approved strong encryption before being sent across the internet. Innovation and Technology can provide guidance on how to securely encrypt an e-mail or download files from the Internet.

- E-mail messages containing confidential information should include the following statement or its equivalent, in all capital letters, at the top of the message:
  "CONFIDENTIAL: UNAUTHORIZED USE OR DISCLOSURE IS STRICTLY PROHIBITED"
- Users must use discretion when accessing voice or e-mail messages with others present. Confidential information should not be left visible while an employee is away from employee's work area. Users should lock their screens when stepping away from their computers.
- E-mail messages sent to or from the City Attorney's office should not be forwarded to any person not originally included in the e-mail transmission list without the express written permission of the City Attorney or his or her designee.
- E-mail, electronic messaging, intranet, voice mail, call history, and Internet/Web access are not automatically deemed confidential and could be subject to public records requests, regardless of whether the device or service is owned by the City if the communication is related to City business. Others outside the City may be able to monitor your e-mail, intranet, and Internet/Web access. For example, Internet sites maintain logs of visits from users; these logs may identify which company, and even which particular person, accessed the service.
- Both the data owner and the recipient of the data are equally responsible for maintaining the classification level of the data as it moves from one party to the other.
- Retrieve all sensitive/proprietary City of Riverside paper records from a copier, fax or printer immediately.
- Users must refrain from discussing City of Riverside sensitive/proprietary information when visitors, consultants, or subcontractors are in the vicinity and are not authorized to receive such information.
- Please refer to *Administrative Manual Policy No. 01.003.00, Confidential Information*, for additional information.

Software Use and Copyrights

- Users are prohibited from installing software on Technical Resources without an IT approved MAC (Move, Add, Change) form.
- Involving IT prior to software installation ensures that the City can properly manage its software, prevent the introduction of computer viruses, and meet its obligations under applicable software license and copyright laws.
- Users may not copy software from the City for personal use.
- Users should not copy or distribute copyrighted or trademarked material (e.g., database files, documentation, articles, graphics files, music, videos and downloaded information) through the e-mail system or any other means unless they have confirmed in advance from appropriate sources that the City has the right to copy or distribute the material.
- Failure to observe copyright or trademark laws may result in disciplinary action against the employee by the City as well as legal action by the copyright owner. Any questions concerning these rights should be directed to the employee's Department Head.
- The City will cooperate with the copyright holder and law enforcement in all copyright matters.

Security

- The City employs various measures to protect the security of its computing resources and its user accounts. Users should be aware, however, that the City cannot guarantee such security. Users should, therefore, engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing passwords regularly.
- Technical Resources are to be accessible at all times by the City. The City, through its Human Resources Director with the approval of the department head, may override passwords,

permissions, or codes to inspect, investigate, or search an employee's electronic files, data, text, images, records, information, and messages on Technical Resources with or without notice.
- Users may not encrypt or encode voice mail, e-mail, or any other data stored or exchanged on Technical Resources using unauthorized methods of encryption.
- The City maintains various network, server, and computer-based security systems to assure the safety and security of the City's networks. Any employee who attempts to disable, defeat, bypass, or circumvent any City security system or device will be subject to discipline up to and including termination.

Security Education

It is the policy of the City to provide periodic security awareness training to all users. Such training will address the new and rapidly changing issues regarding security and the Internet.

New users shall receive an orientation to the Technical Use and Security Policy and additional City security recommendations. Users shall also receive continuous security training in the form of news flashes, security alerts, or tips via newsletters, e-mail alerts, and other appropriate training as determined by the IT department.

E-mail Records and Storage

In conjunction with *Administrative Manual Policy No. 05.001.00, Records Retention and Disposition*, this policy sets forth that e-mail messages are generally considered "transitory" documents (works-in-progress), and, therefore, are not records of the City and are not subject to the City's minimum records retention requirements. The Innovation and Technology Department deletes e-mail in the Inbox and Sent Items folders after 30 days and empties the Deleted Items on a daily basis.

E-mail messages that meet the definition of "public records" as defined in Government Code Section 6252 are maintained by departments based upon departmental records retention schedule. Such records should be moved from the employee's inbox to a subfolder.
- All available e-mails are subject to City's records retention schedules and may be subject to disclosure in response to public records act requests or otherwise. Official Records e-mails must be retained by one of the following means:
    A. Printed out and maintained in the City Department's filing system as a paper document; or
    B. Retained electronically in an organized archival filing system to allow for quick identification and retrieval by IT staff.
- E-mail account size is limited to technical restrictions and available storage. All e-mail messages retained in Outlook subfolders are kept until deleted. This means users must manage their e-mail sub-folders to keep mailbox sizes from exceeding the 50 gigabyte (GB) limit by deleting or printing e-mail messages, based on each department's records retention schedule. Users exceeding this limit will receive a warning message and will not be able to send mail until they have reduced their mailbox size. The Deleted Items folder will be purged daily and is not recoverable.

Policy Violations

- Any user violating this policy may be subject to discipline not limited to revocation of access rights to the Internet, City network, departmental resources, application access rights, or any City technology asset. Also, the City may advise appropriate law enforcement officials of any illegal violations and cooperate in investigations conducted by law enforcement officials.
- City may terminate or revoke access of vendors posing a security risk in violation of City policy.

Responsibilities

- The IT Department is responsible for updating and distributing the Technology Use and Security Policy to the user community and City departments.
- The HR department shall ensure that every employee receives a copy of the Technology Use and Security Policy, and every employee signs an acknowledgement of receipt of said policy.
- Each user of the City's Technical Resources is responsible for understanding and adhering to Technology Use and Security Policy.
- Users are required to retain all public records in accordance with the City's retention policies.
- Users are responsible to report any violations or suspicious activity involving the City's Technical Resources.
- Department heads shall have all volunteers, contractors, or partners granted City Login or network access acknowledge in writing that they have received, read, and understood the Technology Use and Security Policy. The responsible City Director or designee shall also sign this written acknowledgment as the approving authority for granting the user access to City systems. Such written acknowledgment shall be retained in department files.
- Technology Use and Security Policy's Acknowledgment/Receipt form (Appendix A) must be signed by each user prior to granting access to City systems.
- Remote Access Agreement (Appendix B) must be signed by all remote access users prior to granting remote access to City systems. Remote access users must also sign the Technology Use and Security Policy's Acknowledgement/Receipt form (Appendix A).

Disclaimers

- By using City facilities and technology resources, users agree to abide by all related policies and procedures, as well as all applicable law.
- The City specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communication facilities and services, except material represented as an official City record.
- The City makes no warranties of any kind, whether expressed or implied, with respect to the technology services it provides.
- The City is not responsible for damages resulting from the use of facilities, resources and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a City employee, or by the user's error or omissions.
- Use of any information obtained via the Internet is at the user's risk.

Attachments

- Appendix A - Acknowledgment/Receipt Form
- Appendix B - Remote Access Agreement
- Appendix C - Standard Operating Procedure: Vendor Remote Access

Distribution: Regular

APPENDIX A-1

City of Riverside's
Technology Use and Security Policy's
Acknowledgment/Receipt Form

I acknowledge that I have received and read the City of Riverside's Technology Use and Security Policy. I understand the terms of this policy and agree to abide by them.

I understand that I have no right or expectation of privacy in the use of the City's Technical Resources and City Information Systems. I further understand that the City may monitor, review, and log the electronic e-mail messages I send or receive, the Internet address of websites I access, the documents, data, images, voice messages I view, create, save, receive, or transmit, and any network activity including location data in which I transmit or receive files or data using the City's Technical Resources within City facilities or remotely without first notifying me.

I understand that violation of this policy could lead to discipline, up to and including termination, criminal prosecution, and legal liability.

USER

First Name: _____ Last Name: _____

Title / Role: _____

E-Mail: _____

Phone: _____ Mobile: _____

Form Submission Date: _____

Access Start Date: _____ Access End Date: _____

Signature: _____ Date: _____

This form shall be retained in Human Resources Department files.

APPENDIX A-2

City of Riverside's
Technology Use and Security Policy's
Vendor Acknowledgment/Receipt Form

I acknowledge that I have received and read the City of Riverside's Technology Use and Security Policy. I understand the terms of this policy and agree to abide by them.

I understand that I have no right or expectation of privacy in the use of the City's Technical Resources and City Information Systems. I further understand that the City may monitor, review, and log the electronic e-mail messages I send or receive, the Internet address of websites I access, the documents, data, images, voice messages I view, create, save, receive, or transmit, and any network activity including location data in which I transmit or receive files or data using the City's Technical Resources within City facilities or remotely without first notifying me.

I understand that violation of this policy could lead to discipline, up to and including termination, criminal prosecution, and legal liability.

VENDOR

First Name: _____ Last Name: _____

Title / Role: _____

Organization: _____

Address: _____

E-Mail: _____

Phone: _____ Mobile: _____

Access Start Date: _____ Access End Date: _____

Signature: _____ Date: _____

City of Riverside's approving Manager's Name: _____

City of Riverside's approving Manager's Signature: _____ Date: _____

City of Riverside's approving Department Head's Signature: _____ Date: _____

Department Name: _____

For vendor access requests: _____ Date: _____
CIO or Designee

This form shall be retained in Innovation and Technology Department files.

APPENDIX B

City of Riverside's
VPN/Remote Access Agreement

AUTHORIZED USERS ONLY

I am requesting authorization for remote access to the City's Technical Resources and City Information. I understand I will have unique access to sensitive resources that are connected through the City network. To assure security throughout the entire City network, I will actively support and fully comply with the measures described in the Technology Use and Security Policy. I understand that failure to comply can place the entire City network at serious risk; and remote users who fail to comply will be subject to revocation of remote access, network, application rights and or disciplinary action.

Remote users of the City's Technical Resources and City Information shall at all times act in accordance with all applicable laws and City policies, rules or procedures. Remote users shall not use or view City Technical Resources and City Information in an improper or unauthorized manner, and must have a City-business reason do to so.

I have read, understand and am fully aware of the terms of the City of Riverside's Technology Use and Security Policy, especially as applied to remote users of the City's Technical Resources and City Information; and I agree to comply with the terms of this policy. I also agree to remain informed of and comply with future revisions to this policy.

USER

First Name: _____ Last Name: _____

Title / Role: _____

Organization: _____

Address: _____

E-Mail: _____

Phone: _____ Mobile: _____

Access Start Date: _____ Access End Date: _____

Signature: _____ Date: _____

City of Riverside's approving Manager's Name: _____
City of Riverside's approving Manager's Signature: _____ Date: _____
City of Riverside's approving Department Head's Signature: _____ Date: _____
Department Name: _____

For vendor access requests: _____ Date: _____
Information Security Officer

For vendor access requests: _____ Date: _____
CIO or Deputy CIO

This form shall be retained in Innovation and Technology Department files.

APPENDIX C

STANDARD OPERATING PROCEDURE: VENDOR REMOTE ACCESS

Purpose

To provide staff and vendors with protocols regarding requesting and granting remote access for vendors or contractors.

In order to protect City infrastructure, the City of Riverside requires dual factor authentication (Password + Pin) for all remote users.

Scope

- This document applies to all Vendors, Contractors and their employees with remote access to City resources.

Requirements

- Vendor must have existing valid contract with the City.
- Vendor must satisfy the City's Cyber security liability insurance requirements or general liability insurance requirements.
- Vendor and each remote access employee must accept, sign and return the City's Technology Use and Security Policy.
- The request must be approved by the leading department head and the Chief Innovation Officer (CIO) or his/her designee and the Information Security Officer (ISO).

Responsibilities

- Vendor's Internal City liaison will ensure that the vendor has an approved current contract and provide the vendor with copies of the City's Technology Use and Security Policy.
- Vendor's Internal City liaison will obtain the required signatures of the department head and the CIO or his/her designee and the ISO and forward the request to the client services group for provisioning.
- Network and operations teams will provision active directory, remote access request and dual factor authentication and communicate with the Vendor's City liaison.
- Internal City liaison is responsible for project closure notification, documentation and requesting the termination of vendor access upon the completion of the project

Procedure

- Vendor will read, agree to and sign Riverside Technology Use and Security Policy.
- Vendor's internal City liaison will obtain the required approvals and route the request to the client services team.
- Network and operations team will coordinate account creation and remote access provisioning
- The vendor will be assigned a token valid for a maximum of 14 days unless granted an exception through their internal City liaison. After the initial authorization, the vendor will need to request additional access through their City Liaison, which must be approved by the CIO or his/her designee and the ISO.
- Remote access will reset every 4 hours or disconnect after 30 minutes of inactivity, whichever comes first.
- The vendor will only be granted unescorted access to the relevant test or development servers. Unescorted access to production systems is prohibited. Any exceptions require express permission of the CIO.
- Each vendor employee will be assigned a password and will request a one-time pin.
- The remote access password is composed of the combination of the password directly followed by one-time pin
- Server access is granted based on assigned username and password.

- Signed request documentation and request must be uploaded to The Hive with an expiration date.
- Internal City liaison will submit a request to the Innovation and Technology Department requesting to disable vendor's remote access and notify the vendor when the vendor's contract expires or upon the completion of contractual or consulting work.
- If the vendor requests any exceptions to this policy, such exceptions must be justified in writing and approved by the CIO or his/her designee and the ISO.

References

The City of Riverside Technology Use and Security Policy

Definitions

Token: single use randomly generated code provided by an authentication system

Dual Factor: an authentication protocol that requires a combination of something you have (PIN) and something you know (password) to prevent password sharing or theft.

VPN: Virtual private network, encrypted connection granting the remote user access to predefined systems.

Internal City Liaison: City employee managing or coordinating vendor efforts.

Vendor: refers to all Vendors, Contractors and their employees with remote access to City resources.

The Hive: refers to the information system used to track remote access requests.