CITY OF RICHMOND TECHNOLOGY RESOURCE USAGE POLICY

Executive Summary

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at the City of Richmond. The purpose of these policies is to safeguard and protect all technology resources from anything other than authorized and intended use. The main points to remember are:

1. The City provides network, communications systems, equipment and devices ("technology resources") to carry out legitimate City business. By using the City's technology resources, staff consents to disclosing the contents of any data files, information and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment or devices.
2. There is no right to privacy in the use of City technology resources. By using the City's technology resources staff consents to monitoring, recording, and reviewing the use of that technology resource.
3. Users are expected to act lawfully, ethically and professionally, and to exercise common sense.
4. Users who are granted access to critical data are responsible for its protection.
5. Incidental use for personal needs is allowed as long as that activity does not interfere with City business or conflict with any City policy or work rule.
6. Use of technology in violation of this policy is subject to disciplinary action up to and including termination.

1. Scope

1.1. The following policies define appropriate use of the City of Richmond network, computers, mobile computing devices, smart phones, all related peripherals, software, electronic communications, and Internet access. They apply to the access of the City's network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all users of City technology resources regardless of employment status. Access to all networks and related resources require that each user be familiar with these policies and associated work rules. The City of Richmond authorizes the use of computing and network resources by City staff, contractors, volunteers and others to carry out legitimate City business. All users of City computing and network resources will do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules. Technology resources may not be used to facilitate operation of a personal business such as sale of cosmetics, consulting, etc.

1.2. Violations of the Technology Resource Usage Policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination. Additionally, the City may at its discretion seek legal remedies for damages incurred as a result of any violation. The City may also be required by law to report certain illegal activities to the proper enforcement agencies.

1.3. Before access to the Internet via the City network is approved, the potential Internet user is required to read this Technology Resource Usage Policy and sign an acknowledgment. The signed acknowledgment form should be turned in and will be kept on file in the Human Resources Department. For questions on the Technology Resource Usage Policy, contact the Information Technology Department.

2. Ownership of Data

2.1. The City owns all data, files, information, and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment and devices (including e-mail, voicemail, text messages and Internet usage logs even if such communications resides with a third party provider) and reserves the right to inspect and monitor any and all such communications at any time, for any business purpose and with or without notice to the staff. The City may conduct random and requested audits of staff accounts (including accounts with commercial or other third party providers if used in the course of conducting City business) in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist Departments in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the City. Internet, e-mail, voicemail, text message communications and Internet usage logs may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The City's Internet connection and usage is subject to monitoring at any time with or without notice to the staff. There is no right to privacy in the use of City technology resources.

3. Personal Use

3.1. Technology resources may be used for incidental personal needs as long as such use does not result in or subject the city to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City's reputation or credibility, or conflict with the intent or requirements of any City policy or work rule. Incidental personal usage should generally conform to limits typically associated with personal phone calls. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense should be exercised while using City technology resources. Please note that any data stored on City systems including but not limited to email, word documents, and photos may be subject to public disclosure requests.

4. Internet/Intranet Usage

4.1. This technology usage agreement outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed under this section, but there is no right to privacy in staff's use of the Internet/Intranet. Staff Internet usage is monitored. Upon request, Web Usage Reports are provided to Directors to help them monitor their staff's use of the Internet.

4.2. Use of the Internet, as with use of all technology resources, should conform to all City policies and work rules. Filtering software will be used by the City to preclude access to inappropriate web sites unless specific exemptions are granted as a requirement of work duties (e.g., police have the ability to access sites on criminal activity, weapons etc.). Attempts to alter or bypass filtering mechanisms are prohibited. When it is available City resources should be used for Internet access. Staff using City equipment should not use other outside services, directly or indirectly, to bypass web filtering and monitoring.

4.3. Except for City business related purposes, visiting or otherwise accessing the following types of sites is prohibited:

- "adult" or sexually-oriented web sites

- Sites associated with hate crimes or violence
- Personal dating sites
- Sites that would create discomfort to a reasonable person in the workplace
- Any ordering (shopping) of items or services on the Internet.
- Playing of any games

Other activities that are strictly prohibited include, but are not limited to:

- Accessing City information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the City.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.
- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the Information Technology Department and the user's manager.

4.4. The City recognizes that public Internet communications technologies (Web 2.0) are effective tools to promote community and government interaction and that staff want to participate in public communication via blogging, discussion forums, wikis, mashups, social networking, message boards, e-mail groups and other media that are now commonplace tools by which people share ideas and information. However, since activities on public Internet communication sites are electronically associated with City network addresses and accounts that can be easily traced back to the City of Richmond, the following rules must be followed for participation on these interactive public Internet communication sites:

- When expressing staff's personal view, make it clear that it does not necessarily represent the views of the City of Richmond. Opinions or views other than those reflective of City policy must contain the following disclaimer: "The content of this electronic communication does not necessarily reflect the official views of the elected officials or citizens of the City of Richmond."
- Always protect the confidentiality, integrity, and availability of all critical information.

- Staff must not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to or of any other staff, person, and/or entity.
- To protect staff's privacy and the privacy of others, phone numbers or email addresses must not be included in the content body.
- Public Internet communications activity should contribute to staff's body of work as an employee of the City and must not interfere with or diminish productivity.

5. Wireless Communication Device Usage

5.1. Wireless communications devices include, but are not limited to, cellular telephones, wireless handheld devices and pagers.

5.2. A staff's personal communications using City wireless communications devices should be limited, and staff is expected to exercise sound judgment in both the duration and frequency of such use. These devices should not be treated as if they were the staff's personal property. As with similar City property, such as telephones, although minor personal use of wireless communications devices is not prohibited by this policy, it must not interfere with the performance of the staff's work duties or normal business operations of the City. Staff must reimburse the City for costs that would not otherwise have been incurred by the City resulting from the staff's personal use of such devices.

5.3. The City reserves the right to monitor the use of all City-owned wireless devices to the extent they involve City business or are made during the staff's scheduled work time.

5.4. Staff should recognize that wireless transmissions are not secure; thus, staff should exercise discretion when relating confidential information during wireless transmissions.

5.5. Service charges are incurred by the City for the use of optional services such as directory assistance, direct connection by directory assistance, busy signal confirmations, and emergency interrupts. As such, the use of these services on City-issued wireless devices is restricted for business purposes only and should be used only when absolutely necessary.

5.6. Unless authorized, text messages are not to be sent or received. If a text message is received that is not authorized you will need to inform the sender to cease sending such text messages. If text messages are part of the staff's business needs and are authorized, a text message plan should be coordinated with the Information Technology Department to determine the best, most economic plan that will meet monthly needs.

5.7. Unless authorized, any enhanced service such as text, data, picture, ringer tones, mobile applications, downloading of songs or internet not included in the basic plan shall not be permitted on a City-issued wireless device.

5.8. Staff issued wireless devices with a camera feature shall not use the camera feature except in a work related emergency, or as authorized by the staff's department head. The camera feature is not to be used for personal purposes.

5.9. It is at the discretion of the department head and/or City Manager to authorize the replacement/upgrade of City-issued wireless devices. Staff assigned a City wireless device must

be diligent in the care and protection of the City asset entrusted to them. Staff may be responsible for replacement if loss or damage to wireless devices is the fault of the staff.

5.10. In the event of a lost, stolen, or damaged phone it is the responsibility of the staff to report the incident immediately to their department head. The department head then has the responsibility of reporting the incident to the Information Technology Department and the City Manager.

5.11. Use of personal devices for City business is discouraged. Prior approval from the department head or City Manager, whichever is applicable, shall be given in writing by using the "Technology Usage Resource Agreement" (see Appendix A). While on duty or in the work environment, staff must use their personal devices in a professional manner. Staff acknowledges that the use of personal devices for City business could result in their records and devices being subjected to open records requests. **Under no circumstances will the City be held liable or responsible for personal wireless devices used during work hours, even when used for conducting City business.**

5.12. Use of personal devices during work hours for personal use should be limited to emergency uses only.

5.13. **Unless using a hands free device for voice communications, the use of any wireless device while operating a City vehicle is prohibited.** Emergency services personnel are exempt from the law when operating an authorized emergency vehicle. This policy does not apply to persons using their cellular phone to contact law enforcement or public safety agencies for emergency purposes.

6. E-Mail Usage

6.1. E-mail content must be consistent with the same standards as expected in any other form of written (or verbal) communication occurring in a business setting where documents are subject to public disclosure.

6.2. Users must manage their e-mail in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office.

6.3. Use of any globally available distribution lists, such as "City Employees" or "Board of Commissioners", is restricted to the City Manager's Office, Department Directors and their specific designees. Under no circumstances should staff use these lists without prior written consent from their Department Director.

6.4. External mass distribution e-mails to 25 or more recipients are prohibited from City e-mail accounts. Staff communicating to distribution lists of 25 or more recipients should contact the Information Technology Department to have a global list created.

6.5. The City provides staff access to and support of the e-mail messaging system selected by the Information Technology Department. Access or usage of any other messaging systems is not allowed. Subject to the personal use limitations explained above, staff may access web-based personal email but should not download personal documents or attachments from these sites. Staff may not install client based software such as AOL for internet service on city equipment.

6.6. Users should be attentive to e-mails that have unusual or questionable subject lines or content to mitigate spam, phishing and script born viruses that come into the network through e-mail attachments or by clicking on links that lead to hostile web sites. If you suspect phishing or script born viruses in email attachments immediately contact the support desk.

6.7. The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening and having no legitimate or lawful purpose or contents falling within the inappropriate categories for internet usage is prohibited.

6.8. Forwarding of non-work related e-mails, (e.g. “chain letters”, large attachments, audio files, jokes, personal photos, etc.) is strictly prohibited.

6.9. Information Technology Department assigned email addresses should be used for all City related business. Use of personal e-mail accounts for City related business is strongly discouraged. Staff acknowledges that use of personal accounts for City related business may result in their personal data being requested as a result of subpoena and/or open records request. Automatic forwarding of city assigned e-mail addresses to other non-city email addresses is not permitted unless approved by the City Manager and Information Technology Director.

6.10. Upon termination of employment, city assigned e-mail addresses will be closed immediately. Any data currently on the server will be retained for no more than thirty (30) days from termination at which time it will be permanently removed from the e-mail messaging system. It is the responsibility of the department head to request access to the data or to request an extension to retain the data prior to the removal date.

6.11. Staff are required to check their city assigned e-mail accounts on a regular basis. Any accounts that have not been accessed in more than 45 days are subject to be automatically closed and the contents permanently removed unless prior arrangements have been made with the Information Technology Department.

6.12. Staff are required to remove all City e-mail accounts and/or data from any personal devices immediately upon separation from the City.

6.13. Unnecessary e-mail messages and/or attachments should be removed from accounts on a reasonable basis. Unread messages older than 30 days or messages in the Inbox that are more than one year old are subject to be removed at the discretion of the Information Technology Department for the purposes of conserving storage space on the server. Messages that need to be retained beyond 30 days should be placed in a folder other than the Inbox.

6.14. Staff understand that by default electronic mail is not an encrypted service. At no time should critical information, as defined in Section 7.2, be transmitted in part of an un-encrypted message.

7. Security

7.1. The Information Technology department must authorize all access to central computer systems. Each user is responsible for establishing and maintaining a password that meets City requirements as described in the City's Password Policy (Appendix B) for each system as required. The use of another user's account or attempt to capture other users' passwords is prohibited. Each user is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended. Staff who discover unauthorized use of their accounts must immediately report it to the Information Technology Department.

7.2. The City of Richmond will take the necessary steps to protect the confidentiality, integrity, and availability of all of its critical information. Critical information is defined as information which if released could damage the City financially; put staff or citizens at risk; put facilities at risk; or could cause legal liability. Examples of critical data include: staff health information, social security numbers, credit card holder information, banking information, police crime investigation information, etc.

7.3. Staff with access to critical information are responsible for its protection. Staff must take reasonable steps to ensure the safety of critical information including: avoid putting critical data on laptops; encrypting data any time it is electronically transported outside the City network; not storing, saving, or transmitting critical data to a home computer or other external computer; ensuring inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it.

7.4. Staff should not transport critical City data on unencrypted devices such as thumb drives, CD's, or Smartphones.

7.5. Information Technology Department approval is required prior to moving any and all physical media containing critical data from a secured area.

7.6. The City will restrict access to critical information only to staff that have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and ensuring that access to it is limited.

7.7. Staff will be assigned unique user IDs and passwords for network access. Access to systems and applications containing critical information will only be allowed via unique user IDs. Access will be monitored and actions will be traceable to authorized users.

7.8. Staff is prohibited from sharing their passwords or allowing anyone else to use their network account for any reason.

8. Network Access and Usage

8.1. The Information Technology Department must approve connecting devices to the City's network. This includes PCs, network hubs and switches, printers, handhelds, scanners, remote connections, and wireless or wired devices. The use of personal routers and wireless access points on the City network is not allowed.

8.2. The installation, removal, or altering of any software on City-owned equipment is prohibited without authorization from the Information Technology Department or designee.

8.3. Smart phones (Internet and/or e-mail capable cell phones) must meet and adhere to the current standards for those devices as established by Information Technology Department. Personally owned smart phones may be connected to the City's network after Information Technology Department approval. This approval will only be granted after verification that the phone meets City standards and staff have signed the "Technology Usage Resource Agreement" (see Appendix A). Staff agrees that by connecting to the City's email system they are granting the right for the City to remotely wipe all data from the device. **At no time will the Information Technology Department provide support for personally owned smart phones or wireless devices.**

8.4. Exploiting or attempting to exploit any vulnerability in any application or network security is prohibited. Sharing of internal information with others that facilitates their exploitation of a vulnerability in any application or network security is also prohibited. It is also prohibited to knowingly propagate any kind of spyware, and/or denial of service attack or virus onto the City network or computers. Staff who encounter or observe vulnerability in any application or network security must immediately report it to the Information Technology Department.

8.5. Staff must follow the privacy and rules governing the use of any information accessible through the network, even if that information is not securely protected.

8.6. Non-City staffs (e.g. vendors, contractors) are required to have their personal computers scanned by the Information Technology Department for virus detection prior to connecting to the City's network. If the personal computer is going to continue to be connected (even occasionally) to the City's network it must be scanned a minimum of every 30 days. Representatives of the contracting departments are responsible for assisting their contractors to engage the Information Technology Department to perform these services.

8.7. Disabling, altering, over-riding, or turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden. This includes the installation of any software designed to circumvent security measures.

8.8. Because of band-width limitations inherent in any network system, use of the City's network to download non-business related information is prohibited. Examples include streaming video of baseball games, streaming audio of radio programs, MP3 files, online games, etc.

8.9. Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to staff and the City of Richmond.

8.10. Users must manage their electronic documents in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office. Documents past their retention schedules should be deleted from the network to conserve storage space, eliminate the need to backup unnecessary files and to eliminate the opportunity for exposure of personal information.

8.11. Access to the City's network via VPN requires approval from the Information Technology department. VPN accounts will be audited quarterly. Accounts not actively being used will be deactivated or removed. Reactivation of intermittently used VPN accounts for vendor support purposes will be accommodated upon request. VPN users must have commercial up-to-date anti-virus software. Vendors accessing the City network via VPN must adhere to any rules or stipulations put forth by the Information Technology Department. **Only VPN access is provided, at no time will the Information Technology Department provide technical support for non-City owned equipment or devices.**

8.12. At least annually, departments need to review and approve network accounts and accounts for their applications. The Information Technology Department will assist as needed in doing these reviews.

8.13. Unless prior arrangements have been secured with the Information Technology Department, accounts not actively being used, regardless of system, will be deactivated and removed if not accessed at least once every 45 days. All data pertaining to said accounts will be permanently removed 30 days after closure.

9. Administration, Reporting and Violations/Discipline

9.1. Each Department will designate specific staff that has the authority to authorize the Information Technology Department to provide accounts and access to technology resources. Suspected violations or concerns should be reported to the Information Technology Department immediately.

9.2. The Information Technology Department in conjunction with all other Departments share responsibilities in enforcing the Technology Resource Usage Policy as follows

9.2.1. Information Technology Department

a) Responsible for recommending guidelines that are enforceable.
b) Responsible for enterprise monitoring of technology resources using security and monitoring tools. Security and monitoring information will be provided to Departmental Directors as requested to support the investigation of policy violations.
c) If, in the normal course of business activities, the Information Technology Department discovers violations of policy, they will report the activities to the staff's supervisor, Director of HR, and/or to the City Manager depending upon the severity of the infraction.

9.2.2. All other Departments Responsibilities

a) Departments assist in the development and adoption of the Technology Resource Usage Policy.
b) If, in the course of normal business activities, department management suspects staff has or is violating the policy they must report the suspected infractions to the Information Technology Department for further investigation.
c) Departments, Human Resources and City Manager are responsible for carrying out any disciplinary actions in response to violations.
d) Assist in education and communication on an ongoing basis.

e) Departments may develop and implement their own Technology Resource Usage Policy but they will be considered in addition to, at no time will supersede this policy.

9.3. As with any set of policies or rules, exceptions may be granted and documented on a case-by-case basis. These require authorization from the Department involved as well as from the Information Technology Department. Some exceptions may also require City Manager approval.

9.4. Violations of the Technology Resource Usage Policy, work rules, or otherwise inappropriate use of technology resources are subject to disciplinary action up to and including termination. Actions that demonstrate a clear disregard for these policies and requirements and either resulted or could have resulted in damage or serious disruption to the City's network, systems, services, or data; or either resulted or could have resulted in damage to the City's credibility or reputation with the public may result in immediate discharge.

9.5. Internet access, network access and email access will be discontinued upon termination of staff, completion of contract, end of service of non-staff, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

CITY OF RICHMOND
TECHNOLOGY USAGE RESOURCE AGREEMENT

EMPLOYEE NAME _____ EMPLOYEE ID # _____

DEPARTMENT _____

I do hereby acknowledge, understand and certify the following:

- I have reviewed and agree to all the provisions set forth in the City of Richmond Resource Technology Usage Policy.
- The most current version of the City of Richmond Resource Technology Usage Policy is on file with my Department Head, the Human Resources office, and the City of Richmond website. It is my responsibility to keep apprised of all changes to the policy.
- I understand that violation of this policy can result in disciplinary action up to and including termination of employment.
- Upon termination of employment I agree to return all City owned equipment to my supervisor in good working order.
- I understand the risks involved in using personal devices for City business. I further agree that I will not use my personal devices for City business unless prior approval has been given by my department head and the City Manager. I understand the City will not provide any compensation for the use of nor be liable for damages or loss of my personal devices. I agree to immediately and permanently remove all City owned information from any personal devices upon separation from the City.
- A signed copy of this agreement will be kept on file in the Human Resources Department.

EMPLOYEE SIGNATURE _____ DATE _____

Employee has been authorized the use of personal devices for conducting City business.

DEPARTMENT HEAD _____ DATE _____

CITY MANAGER _____ DATE _____

CITY OF RICHMOND
TECHNOLOGY USAGE RESOURCE AGREEMENT
PASSWORD POLICY ADDENDUM

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of City of Richmond's resources. All users, including contractors and vendors with access to City of Richmond systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City of Richmond facility, has access to the City of Richmond network, or stores any nonpublic City of Richmond information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

4.1.2 Users must not use the same password for City of Richmond accounts as for other non-City of Richmond access (for example, personal ISP account, option trading, benefits, and so on).

4.1.3 Where possible, users must not use the same password for various City of Richmond access needs.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

4.1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

4.1.6 Password Creation Guidelines

All passwords should meet or exceed the following guidelines

- Contain at least eight alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).
- DO NOT use words that can be found in a dictionary, including foreign languages, or exist in a language slang, dialect, or jargon.

- DO NOT contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- ARE NOT some version of “Welcome123” “Password123” “Changeme123”

4.2 Password Change

4.2.1 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least an annual basis.

4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every four months. Passwords may not be used more than once in a twelve month period.

4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the Information Technology Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential City of Richmond information.

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not share City of Richmond passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.4.5 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple

words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules that apply to passwords apply to passphrases.

5 Policy Compliance

5.1. Compliance Measurement

The Information Technology Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Information Technology Department in advance.

5.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.