CITY OF SAN RAFAEL
POLICIES AND PROCEDURES

Policy No.	110-01
Subject:	Computer Use and Security
Resolution No.	N/A
Issue Date:	December 1, 2005
Revision Date:	September 13, 2013
Prepared By	Gus Bush, IT Manager
Approved By:	Nancy Mackle, City Manager

PURPOSE:

The City of San Rafael recognizes that maintaining the integrity of the City's computer systems and the protection of data and confidential information contained on those systems is vital for the efficiency, cost-effectiveness, and quality of work generated by City employees and contractors. The increasing use of the Internet and the proliferation of technological advances in the field of computers have significantly improved the communication, research, and work product of the City, albeit at the increasing risk of exposing the City's computer systems and data stored on those systems to damage caused by external sources, viruses, computer contaminants and unauthorized users. Therefore, the City must impose a policy to prohibit the usage of the City's computer systems and network which would undermine the integrity of the system, data and confidentiality of information contained on the systems and tend to impair job performance, efficiency or productivity.

RESPONSIBILITY:

All City Departments, Divisions, and City Officials

REFERENCES:

Social Media Use Policy
Virtual Private Network Service Agreement
Web Site Management Policy
Website Link Policy
Wireless Communications Policy

POLICY

The City's computer system (including all hardware and software) are the exclusive property of the City and are provided to employees and contractors for creating and transmitting City business-related information. The City treats all computer files, including electronic messages sent, received, and retained, as City business information.

1. Access Controls

Requests for new network accounts will be documented in writing and submitted to the Information Technology (IT) office for processing. Once a network account is established, requests for access to specific departmental systems may be made directly to the assigned system manager.

Departments will notify IT when accounts are no longer needed, before departure or as soon as feasible afterwards. Accounts will be disabled (or passwords changed) immediately upon departure (or notification afterwards). Departments will have at least 30 days to determine disposition of new/remaining files/messages prior to account deletion.

Accounts for temporary staff and contractors will remain active for no more than 180 days, without express approval by the IT Manager. Each extension for additional 180 day periods will be documented.

Shared user accounts may be established in certain circumstances, with prior approval from the IT Manager.

Two factor authentication (such as biometrics, electronic tokens, etc) may be employed in situations where enhanced security is desired or required by outside agencies.

Systems will display logon banners that provide information about security and privacy policies.

2. Remote Access

All employees and contractors are eligible to apply for remote access to the City network. Authorized applicants must sign and adhere to the Virtual Private Network Service Agreement. The City reserves the right to revoke individual remote access at any time.

Remote access to City systems will be established only with IT Manager and/or Department Director level authorization.

Tools used to remotely access City systems will only be activated from within the City network, not activated remotely from outside the City network. Passwords and/or other appropriate security measures will be employed when using remote access tools.

3. Passwords and Access Codes

Strong passwords will be used for all systems, including a minimum of 8 characters with a combination of upper case letters, small case letters, numbers, and special characters. Passwords will be changed at least every 6 months but not more often than once a month, without administrator intervention. Password histories will be used to not allow them to be repeated within three iterations. Repeated attempts to access the system or network with an incorrect password will require a lock out of at least 15 minutes, without administrator intervention. Screens will be locked automatically after 30 minutes of inactivity.

Authorized individuals may not disclose to unauthorized persons or entities their assigned passwords or access codes for entry into or use of City systems or network. Individuals are prohibited from allowing or assisting unauthorized individuals with access to City systems or network. Further, individuals are prohibited from representing oneself as another individual by some electronic means unless so specifically authorized by that individual and the City Manager or his or her designee.

4. Mobile, Personal, and Other Devices

Mobile devices (such as tablets, smartphones, digital cameras, etc) and portable media (such as optical disks, flash storage, portable hard drives, etc) may be used to access City data and/or transfer files to/from City systems, when required for business purposes. Users and Departments will apply appropriate security, based on the type of data involved.

Personally owned devices (computers, mobile devices, portable media, etc) may be used to access City data and/or transfer files to/from City systems, when required for business purposes. The City retains ownership rights to any data or software stored or transferred to/with personal devices. The City reserves the right to monitor activity on personally owned devices used for business purposes and/or install tools for managing its data or controlling access.

No unauthorized wireless access points, routers, hotspots, voice over internet protocol (VOIP) devices, or similar devices will be installed on the City network. All network access devices must be installed and/or approved by IT.

5. Privacy

The City's computer systems and network are provided to City employees and contractors as tools to assist in performing their official duties. As such, if individuals make incidental use of City systems for personal reasons, they should not expect their data to be protected from review or deletion. The City expressly reserves the right to access, monitor, review, copy and delete all data. Accordingly, individuals should not use City systems to create or transmit information they wish to keep private.

Supervisors may request reports, system logs, and other available information on system usage as needed to evaluate and monitor performance of duties. Such requests shall be submitted to the Human Resources (HR) Director for approval; the HR Director may then forward the request to IT for action.

6. Confidential Information

Individuals must exercise caution when creating or transmitting City confidential business information electronically. Confidential business information may not be transmitted to employees or other individuals who are not authorized to receive such information.

Any correspondence which contains confidential attorney-client information 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 by law.

Medical and/or health related information as covered under the Health Insurance Portability and Accountability Act (HIPAA) will be protected by established policies and related standards.

Individuals will not transmit passwords, credit card numbers, social security numbers, or similar confidential information in the clear.

Only authorized City representatives are permitted to communicate with non-employees on behalf of the City via City systems. If an individual is unsure as to whether a communication is authorized, it is that individual's responsibility to inquire with their supervisor as appropriate.

7. Internet Access and Prohibited Use

The City provides access to the Internet for City business-related purposes. The City has the capacity to filter, monitor and review website traffic and access. Individuals should not have any expectation of privacy regarding the websites accessed through the City's computer systems. Computer systems may "leave tracks" at websites visited. Because of the nature of City business, any incidental use of the Internet for personal use must be conducted with the highest level of professionalism. Individuals must also adhere to any additional department internet access restrictions.

Individuals using City systems are prohibited from intentionally accessing any Internet sites that are discriminatory or offensive in nature, or promote or advocate any form or type of discrimination. Individuals are prohibited from posting personal opinions on the Internet using City systems, without the City Manager's or his or her designee's approval.

Any attempt to access a website that has been filtered by the network website filtering software, or any attempt to bypass the City network filtering measures by the use of software or hardware designed for the purpose of bypassing City filtering measures is prohibited. Should the need arise to access a filtered/prohibited website, individuals should contact his or her supervisor and gain official authorization to have City IT staff allow the necessary access for the prescribed period of time.

City systems may not be used to solicit or proselytize for commercial ventures, religious or political causes, or outside organizations that are not authorized by the City Manager or his or her designee.

8. Electronic Messages

Electronic messages and emails sent or received by City employees or contractors qualify as public records under the California Public Records Act, and will be subject to inspection by members of the public with limited exceptions if the messages concern City business and are kept by City employees or contractors in the ordinary course of business. A message will be

considered to be retained in the ordinary course of business if the individual makes a hard copy of the message for storage in the Departmental files, stores a copy of the message in an electronic repository, or stores the message in an identified subfolder in the employee's electronic mailbox. Copies of messages stored on backup systems solely for disaster recovery purposes will not automatically be considered public records, and may be overwritten or deleted by IT through its standard operating procedures.

If an individual places a message in either the Deleted Items or Sent Items folder in their mailbox, it will be presumed to be not kept in the ordinary course and will not be considered a public record. Messages older than seven (7) days in the Deleted Items folder will be automatically deleted. Messages older than thirty (30) days in the Sent Items folder will also automatically be deleted.

To ensure each employee manages the volume of their electronic messages appropriately, mailbox size limits are in place. A mailbox size is determined by the total disk space necessary to store the mailbox contents, including attachments. When a mailbox reaches 300 megabyte (MB) in size, a warning will be sent to the employee on a daily basis until the total size of the mailbox returns below the 300 MB limit. Additionally, mailboxes reaching 400 MB will be disabled from sending and receiving additional messages until such time as the mailbox size returns below the 400 MB limit.

Since electronic messages stored on City computers will be open for inspection by members of the public including the news media, just like hard copy documents that are placed in the City's Departmental files, individuals are encouraged to include in such messages only such information as is necessary for the purpose of conducting the City's business.

To facilitate efficient use of electronic messaging, the City maintains many distribution lists, including a global list of all City email accounts. The distribution lists are only to be used for official City business. Messages sent using the global distribution list must be relevant to all City employees and be approved by a Department Director. Additionally, individuals must be aware of the message size (including attachments) and strive to minimize the size of messages sent to all City e-mail addresses. Where possible, network drives should be used to share electronic documents rather than sending them via email.

Alternatively, the City maintains an intranet website accessible by City Employees. The intranet is an appropriate place to post documents generally of interest or need by City employees. In addition, a City Employee Bulletin Board is available for individuals to electronically post non-city related information.

9. City Employee Bulletin Board

The Employee Bulletin Board was designed to create a space for employees to post items for sale, make announcements, or share events with fellow employees. Photo albums are also posted of city employee events. Below are several guidelines for posting to the Bulletin Board.

Only city employees may advertise items for sale or post announcements and events to the Bulletin Board.

Pictures of the item(s) may be submitted for viewing.

The following items are NOT ACCEPTABLE:

Items (new or used) intended for resale

Weapons and ammunitions

Pornographic materials/items

Alcohol and tobacco

All other items prohibited by law or other City policy

The City of San Rafael is not responsible or liable for items purchased or sold through the Employee Bulletin Board. The City reserves the right to remove any post at any time.

10. Computer Software

The City has invested significant financial and staff resources into development and maintenance of city-owned computer resources, such as the equipment and software. To protect that investment and to ensure that all software used is properly licensed and registered, all software used on city-owned computers is to be loaded by City IT staff, or with express permission from IT staff.

No personal software is to be loaded on city-owned equipment. No software, except updates from official websites associated with approved virus protection software and updates for approved business software, is to be downloaded from the Internet or other electronic sources without express permission from City IT staff. Any copying or distribution of city-owned software for non-City use is strictly forbidden.

11. Security Awareness Training

Training will be conducted for all new employees (permanent or temporary) and contractors prior to or in conjunction with receiving initial passwords. Refresher training will be conducted as needed on a yearly basis or when major changes to systems or procedures occur. Documentation will be maintained by HR, IT, or departments as applicable.

12. Incident Response

Users will notify IT immediately of any potential security incidents involving the City's network and/or computer systems (including but not limited to compromised passwords, virus/malware activity, unauthorized access, or physical loss/damage to City systems). IT will respond and document its response to potential incidents, determinations made, and corrective actions

taken (if any). IT may establish automated response capabilities for resetting passwords, reporting spam, and similar low-risk situations.

13. Violations
Violations of any provision of this policy by any individual or entity may result in disciplinary action up to and including dismissal and/or civil or criminal prosecution.

APPROVED BY:

Nancy Mackle

Nancy Mackle, City Manager

9/13/13

Date

CITY OF SAN RAFAEL

Virtual Private Network Service Agreement

I. Purpose

This document outlines an agreement for accessing the City of San Rafael's computer network by means of a Virtual Private Network (VPN) connection, within the Computer Use and Security Policy of the City. Remote access to the City network will be appropriately provisioned and/or controlled to ensure required security.

II. Definitions

Virtual Private Network (VPN): A VPN creates a secure connection, called a tunnel, between a client computer and a VPN server or host. This connection is usually made over the Internet and, in that case, has the effect of extending the City of San Rafael network to remote users. Once connected, a user may access files and/or applications stored on central servers just as if the user's machine was connected directly to the City Network at a City facility.

III. Service Terms and Conditions

Approved employees, contractors, and consultants may connect to the City Network via VPN. Approvals must be obtained from the appropriate management at the Department Director level and above as well as the City Information Technology (IT) Manager. Requestors must have a demonstrated business need to connect securely and/or to appear as a part of the City Network. Use of this service in the performance of activities unrelated to the mission of the City is strictly prohibited. VPN is a user managed service. As a result users of this technology are responsible for selecting an Internet Service Provider (ISP), coordinating installation with their ISP of any required software, and paying associated fees.

Additionally,

1. It is the responsibility of those with VPN privileges to prevent unauthorized access to the City Network from their VPN connected computer.
2. Users will be authenticated through their assigned City Network username and password.
3. Users with VPN privileges may only use VPN client software obtained or approved by the City's IT Division.
4. City Employees may only utilize the VPN client from a City assigned and configured computer.
5. All computers connected to City Network **must**:
    a. Use the most current anti-virus protection
    b. Keep computers updated with the latest critical operating systems patches
    c. Use compatible firewall protection.
6. When remotely connected to the City Network via VPN, users agree that they are subject to the same City rules and regulations that apply to on-site usage. In particular, users must adhere to the City of San Rafael Computer Use and Security Policy.
7. All requestors must read and agree to these terms and conditions before a connection is granted.
8. Data collected, stored, backed up, processed or accessed using this service must be protected according to City policies and procedures.
9. Proper data removal/destruction procedure must be followed for off-site systems at the end of employment, any contractual arrangement, or cessation of the individuals VPN service.

IV. Enforcement

All individuals granted access to this VPN service must adhere to the service terms and conditions. If these terms and conditions are violated, VPN access will be revoked. Violations will also be reported to the users' management, which may lead to other disciplinary action up to and including legal action and/or termination.

V. Request for authorization

I have read and agree to the terms and conditions stated above.

Requestor's Signature _____ Signature Date _____

Printed Name _____ Title _____

Department or Company Name _____

Email Address _____ Daytime Phone _____

VI. Approval (INTERNAL USE ONLY)

Dept Director (or designee) _____ Signature Date _____

Printed Name _____ Title _____

Effective Date _____ End Date (if known) _____

IT Manager (or designee) _____ Signature Date _____

Printed Name _____

VPN Granted Date _____ Terminated Date _____