12.3 Information Technology Usage Policy

Purpose

The purpose of the City of Ramsey IT Policy is to set standards to protect the City's IT systems from business interruption, unauthorized or inappropriate access, and maintain appropriate security. The policy is to be adhered by all users (regular, part-time, and temporary employees, vendors, consultants, volunteers, interns, and others) who have access to or uses the City of Ramsey IT systems both on and off City property. IT systems include, but not limited to, computers, e-mail, Internet, printers, software, telephone, voice mail, and others.

Glossary of Terms

Configuration: The way a system is set up or the assortment of components that make up the system. Configuration can refer to either hardware or software or the combination of both.

Downloads: To copy data, usually an entire file, from a main source to a computer device. The term is often used to describe the process of copying a file from an online service or bulletin board service to a computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

Electronic Mail (e-mail): A network application that allows users to exchange messages over communications networks with someone else.

File Server: An enhanced computer with network operating software that is used for file storage, application functionality, and managing network resources.

Information Technology (IT): Managing and processing information.

Information Technology Systems: Includes, but not limited to, computers, printers, software, e-mail, Internet, telephone, voice mail, and others.

Internet: A global network connecting millions of computers.

Intranet: Network base access accessible only within an organization. An intranet 's Web sites look and act just like any other web site, but firewall security restricts unauthorized access.

Local Area Network (LAN) – A computer network.

Licensing: Legal compliancy of assets.

PDA's: Personal Digital Assistants (i.e. Palm Pilots, Blackberrys)

Software: System software includes the operating system and all utilities that enable the computer to function. Application software includes programs that do real work for users (i.e. word processors, spreadsheets, and database management systems).

Portable Equipment: Hardware that is small and lightweight (i.e. laptop computers, hand-held computers, PDA's, projectors, digital cameras).

Users: regular, part-time, and temporary users, vendors, consultants, volunteers, interns, and others.

Auditing

The City of Ramsey reserves the right to monitor and audit use of its IT systems at any time without user's consent. An audit may result in the removal of hardware and/or software not compliant with this policy.

Reporting

Users should notify their immediate supervisor, the IT Manager, the Human Resources Manager, the City Administrator or any member of management upon learning of violations of this policy.

Expectation of Privacy

As a government agency, the City is subject to public disclosure laws. All files and documents, including personal messages and Internet logs, are owned by the City and may be subject to open records requests under law. Users should have no expectation of privacy.

Violation of Policy

Violations of this policy will be addressed consistent with the City's Personnel Policy.

Information Technology Use

Purpose

Inform and provide direction to all users regarding appropriate usage and management of the City's IT systems and resources. All users must be authorized to use City IT systems through user's department head, supervisor, or IT.

Hardware and Software Acquisition

The IT Manager must approve all hardware and software prior to acquisition to ensure consistency with the design and architecture of the City's IT network. Users are prohibited from installing, downloading, or acquiring hardware and software, including product demonstrations, without prior approval from the IT Manager. Software applications not required for official City business are strictly prohibited.

Installation, Downloads, and Configuration

No user will be allowed to manipulate hardware and software standard configurations. The IT department must always be contacted for hardware and software support.

No user should change the computer setup or configuration files. Customizing a computer should be limited to items including City-owned software such as wallpaper, screen savers, icons, toolbars and colors. Users are prohibited from downloading, or installing any software including personal, through the Internet, e-mail, and/or vendor demonstrations without prior approval from the IT department.

Licensing

To ensure license compliancy all software must be purchased by and licensed to the City.

Development**:** Any software programs, i.e., custom designed Microsoft Access databases, developed for use by the City becomes the property of the City. Software programs may not be sold or distributed without prior approval.

Home: City-owned software may not be loaded on non-City owned equipment unless there is prior approval of department head and IT Manager.

Copyright Laws: City users are required to abide by software and documentation copyright laws and licensing agreements. If there is any question about the legality of the software and documentation, it should be directed to the IT Manager. At no time should any users make copies of City-owned software and documentation. To prove legal ownership of software, the City must have the original media and manuals stored on City property. The IT Manager will periodically check for software that may be in violation of the above policy.

Data Management and Protection

Under the provisions of the Minnesota Data Practices Act, all data stored on computer media owned, leased or rented by the City is considered to be owned by the City and for the most part is non-private/public, including information stored on local hard drives. Data is subject to the Minnesota Data Practices Act and its use and dissemination is consistent with the data classification under the Minnesota Data Practices Act. This data is also subject to review and investigation at the discretion of the City Manager, department heads, IT Manager, and/or law enforcement. The City Clerk should be contacted with questions regarding the classification of public and private data.

Data Ownership: All information developed or introduced to a City technology system by a user in conjunction with employment with the City is the property of the City.

Data Storage: All City data must be saved to a network drive on a City server.

Users are responsible for deleting outdated files that are no longer needed for the compliancy of the City Records Retention Schedule; this includes data files and e-mail messages. The Assistant City Administrator should be contacted with questions regarding the City Records Retention Schedule.

Data Back-up: The IT department backs up all data stored on the file servers. Workstation hard drives or any other devices are not backed up.

Portable files: To facilitate off-site work, users may copy appropriate files to and from diskettes/CDs including word processing, spreadsheets, and presentation graphic files. No other files or information may be copied to or from the City computers. A current copy of the portable file(s) must be maintained on the City server.

Password Protection: If any software product that the City has purchased has the option to have files password protected, the password must always be shared with the appropriate management personnel and/or the IT Manager.

Portable Information Systems

Portable personal computer(s), digital cameras, projectors, and other City owned portable equipment can be used for City business, outside of City facilities. When users check out portable equipment they are expected to provide appropriate "common sense" protection against theft, accidental breakage, environmental damage and other risks. Desktop computers and attached devices are not to be removed from City buildings. The user is responsible for the back up of or loss of any data stored on the standalone or portable computer. IT staff is available to assist in the development of procedures for disaster recovery of portable units.

Personal Digital Assistants (PDA)

Users acting within the scope of their job responsibilities and with department head approval, may personally purchase a Personal Digital Assistants (PDA's) from an IT approved and published list of brands and models. IT staff will install approved PDA's on City owned equipment. The city may at its discretion provide PDA/Blackberry devices to members of staff it deems appropriate.

Electronic Mail (e-mail)

The City e-mail system is a tool to be used for matters directly related to the business activities of the City and as a means to provide services that are efficient, accurate, timely and complete. E-mail messages are subject to regulation under the Minnesota Data Practices Act. The content of the message determines whether a message is public or non-public/private. E-mail is intended as a medium of communication, not for information storage; therefore, e-mail should not be used for the storage or maintenance of official City records or other City information. Users may receive inappropriate and unsolicited e-mail messages. Any such messages should be reported immediately to the IT department.

Inappropriate non-business use of the City e-mail system includes, but is not limited to; the transmission of non-business audio, graphic or movie files (to include streaming audio and video, MP3, Jpg, Tif, Gif, Mpg, AVI etc.); games; jokes; instant messaging; content of an offensive or pornographic nature; copyrighted material and large data files not directly related to [City Name] business. These items must not be sent or accepted as e-mail attachments. These types of files can be large and affect the network or computer performance or carry viruses.

The City retains the right to use management software to eliminate the delivery of junk e-mail (SPAM), including e-mails that contain profanity.

Internet

The Internet is available to users for research, education, and communications directly related to the mission, charter, or work tasks of the City. Users must honor copyright laws regarding protected commercial software or intellectual property. Users of the Internet should minimize unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource. Use of the Internet through City computers is a privilege, not a right, which may be revoked at any time for abusive conduct. Users are responsible for adhering to City standards when browsing the Internet. Failure to adhere puts the City and the individual at risk for legal or financial liabilities, potential embarrassment and other consequences.

The City retains the right to use management software to monitor end user activity. This software may monitor and limit Internet activity in order to ensure the most efficient use of the valuable resource.

Prohibited Use

Use of City IT systems is strictly prohibited at all times for:

- illegal activities
- profit or commercial activities
- any other public office or employment which is incompatible with City employment

responsibilities, as determined by the City Administrator

- wagering, betting, or selling chances
- annoying or harassing other individuals
- fund-raising, except for City approved activities
- any political or religious activities
- unethical activities

Personal Use

The City of Ramsey offers users the privilege of personal use of its technology. Recognizing that users will benefit from practice using technology, personal use is allowed using the following guidelines listed below:

- Users must obtain approval from their immediate supervisor prior to personal use of IT systems
- Only City users are to use the computers and computer related peripherals
- Personal use is permitted only before and after regular business hours and only when other City business is not to be performed on the systems

- Users must use their own media (disks, CD's) and paper. No personal files or data are to be stored on the City file servers
- Users must not use IT systems for items listed above in Prohibited Use

E-mail: E-mail may be used for personal correspondence, as long as it does not interfere with the normal duties of the employee and the above-listed guidelines are followed. Using the City Internet e-mail to participate in any kind of non-business related listservs or broadcast mailing list is prohibited.

Inappropriate non-business use of e-mail can cause a burden on resources or carry viruses. Examples of this includes, but is not limited to : the transmission of non-business audio, graphic or movie files (to include streaming audio and video, MP3, Jpg, Tif, Gif, Mpg, AVI, etc.); games; jokes; instant messaging; content of an offensive or pronographic nature; copyrighted material and large data files not directly related to business.

Internet: Internet access may be used for personal use as long as it does not interfere with the normal duties of the employee and the above guidelines are followed.

Inappropriate non-business use includes, but is not limited to: audio, graphic or movie files (to include streaming audio and video, MP3, Jpg, Tif, Gif, Mpg, AVI, etc.); games; jokes; instant messaging; content of an offensive or pornographic nature; copyrighted material and large data files not directly related to city business. These items must not be downloaded from the Internet. These types of files can be large and affect the network or computer performance or carry viruses.

Desk Telephones: Desk telephones may be used for personal use as long as it does not interfere with the normal duties of the employee and the above guidelines are followed. In the event that an employee needs to make a personal toll call, the preferred method of payment is a personal calling card. If a situation arises where you do not have access to a personal calling card you must notify the finance department of the date, time and location of where the call was placed. The charge for the call will be the actual charge, plus tax, that would normally be incurred by the City. Payment is due within 7 days after receipt of the long distance bill.

Copiers, Fax Machines, Printers: Users will reimburse the City of Ramsey for personal copies, faxes, and print requests, at the rate listed in the City fee schedule. Personal use fees must be reimbursed within 24 hrs from the date the expense was incurred.

Information Technology Security

Purpose

Ensure secure, protect, and allow appropriate access to City of Ramsey IT systems and resources.

Logins and Passwords

All users must use and maintain unique IT-issued login IDs for computer and network-related access. Login IDs are not to be shared with others, and corresponding passwords must remain confidential. Multi-user or generic login IDs are permissible only in special circumstances approved and maintained by IT. User passwords must adhere to the following requirements:

- Have a minimum of at least six alphanumeric characters in length
- Must be changed every 180 days
- Have at least one numeric digit as well as letters, for example: jarg0n5
- Have not been previously used in the last three password rotations

Appropriate network access shall be assigned by the IT department to each user login ID, and users may only log into computers and equipment with their assigned login ID. Passwords are not to be shared with anyone, and will be forced to change periodically. New passwords should not be easily guessed. Any employee who forgets their password or suspects that their password's security has been compromised, may contact the IT department to be issued a new one, which must then be changed immediately.

Physical Security

City users are expected to provide reasonable security to their computer workstations and related IT equipment. This includes ensuring that passwords are not written down in accessible places, removable media must be kept in a secured area, and that confidential data is not displayed in such a manner that unauthorized personnel can view it.

All IT equipment is City property and must remain on current premises. Users may not move IT equipment outside of its assigned area without prior approval from the IT department. Designated portable equipment, such as projectors, laptop computers, and digital cameras, may be removed from City buildings only for City business. Portable equipment must be reserved and checked out only to City users. Users are expected to provide appropriate "common sense" protection against theft, breakage, environmental damage, and other risks.

Users are required to log off computer workstations when absent for an extended time, such as end of day. Users may, however, "lock" their workstation instead when absent for a short period of time, such as during a meeting or over lunch.

Virus Protection

All computer workstations, laptops, and servers must be protected from viruses using up-to-date antivirus software. Users may not alter their system's configuration or take other steps to defeat virus protection devices or systems. All files on removable media must be scanned for viruses prior to installation onto or access from City computer equipment. Any files suspected or known to contain viruses must be immediately reported to the IT department for proper handling.

Remote Network Access

Remote access is defined as the ability to connect to a computer or network from a distance, such as from home, hotel, conference, Internet kiosk, etc. Remote access into the City's network, or any City-owned device, may be granted upon meeting the following conditions:

- Business-related purpose approved by requesting department head and IT Manager.
- Use of industry standard encryption and/or City supported VPN (Virtual Private Network) technology.
- Authentication and access control will be maintained via the City's domain. Valid network login and passwords are required.
- While remotely connected, nobody but the authorized user may have access to the computer making the connection.
- Remote computer must comply with current anti-virus and security parameters as specified by the IT department.

All remote users are subject to the rules and regulations set forth in this entire policy for all network users. Users should follow proper data practices protocols as directed by the Minnesota State Statutes. Storing of business related information on a home computer creates an extension of the member's network; thus anything stored on that computer, might be subject to public data requests.

Wireless Access

Unauthorized wireless access into the City's computer network is strictly prohibited. Wireless access is defined as, but not limited to, 802.11 (Wi-Fi), Bluetooth, WiMax, and cellular technologies. Users may not attempt to scan, connect to, or install any wireless computing device on City equipment or property. Wireless access must be authorized and configured by the City's IT department. Any authorized wireless access must utilize standards-based encryption, and conform to adopted security practices as governed by LOGIS and/or state and federal government guidelines.

12.6 Cellular Phone Policy

PURPOSE

This policy is intended to define acceptable and unacceptable uses of city-provided cellular telephones. Its application is to ensure that cellular phone usage is consistent with the best interests of the City without unnecessary restriction of employees in the conduct of their duties. This policy will be implemented to prevent the improper use or abuse of cellular phones and to ensure that City employees exercise the highest standards of propriety in their use.

POLICY

Cellular telephones are intended for the use of City employees in the conduct of their work in the service of Ramsey citizens and businesses. Department heads are responsible for the cellular telephones assigned to their departments, determining service levels for their employees, and exercising discretion in their use. Employees will manage their cell phone use so as not to exceed their service level as approved by their supervisor. Occasional overages will be reviewed by the supervisor on a case by case basis. After a review of the monthly billing statement, employees may be required to reimburse the City for overages in cell use, depending on the nature of the calls made during the month. Employees will make an effort to utilize the Nextel Direct Connect and/or a land line before utilizing cellular minutes. Nothing in this policy will limit department head discretion to allow reasonable and prudent use of such telephones or equipment provided that:

1. Its use in no way limits the conduct of work of the employee or other employees.

2. No personal profit is gained or outside employment is served.

A department head may authorize an employee to use their own personal phone for City business and be reimbursed by the City for those calls. An employee will not be reimbursed for business-related calls without prior authorization from his or her department head. Department heads may also prohibit employees from carrying their own personal cell phones during working hours if it interferes with the performance of their job duties.

Use of public resources by City employees for personal gain and/or private use including, but not limited to, outside employment or political campaign purposes, is prohibited and punishable by disciplinary action which may include termination and/or criminal prosecution, depending on the nature and severity of the transgression. Incidental and occasional personal use may be permitted with the consent of the department director and direct supervisor.

Personal calls made by employees on a City-provided cellular phone will be made or received only when absolutely necessary and when they do not interfere with working operations and should be completed as quickly as possible.

PROCEDURES

It is the objective of the City of Ramsey to prevent and correct any abuse or misuse of cellular telephones through the application of this policy. Employees who abuse or misuse such telephones may be subject to disciplinary action under the personnel policy or a collective bargaining agreement.

RESPONSIBILITY

The Administrator, or designee, will have primary responsibility for implementation and coordination of this policy. All department heads and supervisors will be responsible for enforcement within their departments and divisions.

Date Policy Established: 03-2004