City of New Hope
Information Technology Policies

Updated: 12/11/2023

I. Introduction

The city provides computer systems and services to employees and elected officials at the city's expense, for use on city business. The purpose of this policy is to set forth rules and guidelines that shall govern the use of all city computer systems and software. This policy applies to all employees and elected officials who are authorized to use the city of New Hope computer systems, hardware and software. All users are required to abide by the policy, which will be enforced by management personnel.

II. Network

All PCs in the city of New Hope are networked. This allows all PCs to share network resources such as printing, file storage, electronic mail, software and access to the Internet. No city technology may be used for outside employment, including but not limited to the network or individual devices.

A. Security

- All users are required to adhere to the LOGIS Members Security Policy dated 12/1/2023.
- Login names will be assigned and users given rights to, appropriate resources by IT personnel. All login names will follow the naming convention of first letter of the first name, followed by the last name. In the case of duplicate names, the middle initial would follow the first initial.
- All network users will be required to log into the network with a password. Users will be prompted by the network system to change their password every 42 days. All users must keep their user password confidential. Users are responsible for security.
- Password Guidelines:

  All user passwords must follow these specifications:
  - ✓ Contain both upper and lower case characters (e.g. a-z, A-Z)
  - ✓ Contain a digit, symbol character, one upper case and one lower case letters, for example: kep1tSafe#.
  - ✓ Have a minimum of ten alphanumeric characters.
  - ✓ Must not be a word in any language, slang, dialect, jargon, etc.
  - ✓ Must not be based on personal information, names of family, etc.
  - ✓ Have not been previously used.
  - ✓ Must never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation or other phrase. For example: *This May Be One Way To Remember*. The password would be "TmB1w2R!" or "Tmb1W>r~", or some variation.
  - ✓ May not be changed more frequently than once a day.
  - ✓ Must be different than passwords used elsewhere (e.g., personal bank accounts)
  - ✓ Must be changed by the user on the first use.
- Before leaving your workstation, always lock your computer.
- All data should be saved to the network so that it will be backed up and secured if your workstation or data is stolen, vandalized or malfunctions.

III. Software

A. Copyright Laws

- All users are prohibited from making illegal copies of software owned or leased by the city. All copyright laws must be abided.
- Installing software on more computers than the legal license permits will not be allowed.

B. Installation

- All software installation, whether to the server or to the PC, shall be done by IT personnel.
- Installing personally owned software, downloaded software, or free shareware on a city PC is not allowed.

C. Purchases

- Any specialized, work related software must be approved by IT personnel before purchasing.

D. Use

- All users shall refrain from changing the setup or configuration files that control basic computer functioning.

E. Development

- All software programs developed for use by the city become the property of the city. These software programs may not be sold or distributed. This includes, but is not limited to, macros and templates created for word processing, spreadsheets, presentations, and databases.

IV. Electronic Mail

City email 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. Email 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. Email is intended as a medium of communication, not for information storage; therefore, email should not be used for the storage or maintenance of official city records or other city information. Users may receive inappropriate and unsolicited email messages. Any such messages should be reported immediately to the Director of HR and Administrative Services.

Inappropriate non-business use of the city email system includes but is not limited to; the transmission of non-business audio, graphic or movie files (to include streaming audio and video, mp4, jpg, tiff, 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 of New Hope business. These items must not be sent or accepted as email attachments. These types of files can be large and affect the network or computer performance or carry viruses.

All email messages will automatically be deleted from the system 2 years after receipt. If retention of any message is warranted beyond that period, the message should be moved to a permanent storage area such as a department file directory on a city server.

The city retains the right to use management software to eliminate the delivery of junk email (SPAM), including emails that contain profanity.

A. Login Names

- Outlook Mail Login names shall be the same as the network login name.

B. Security

- All users' passwords shall be kept confidential.
- If a password is forgotten, the user account must be reset, so it can be accessed again. This can be done by contacting the help desk.

C. Privacy

- Electronic correspondence is considered private to the extent that under normal circumstances, it is accessible only to the addressee. However, under special circumstances or investigations, email messages sent or received in conjunction with government business may be releasable under the Freedom of Information Law. A general rule is never send correspondence that you would not mind seeing posted on the city bulletin board.

D. Appropriate Use

- No chain letters, advertisements, solicitations or non-business related mass mailings will be allowed.
- Personal use of email should be kept to an absolute minimum.
- All users are required to save hard copies or text files of all critical email correspondence. Note: Deleted email messages can often be retrieved.
- Harassing or threatening messages are prohibited.
- Any effort to conceal the sender's identity or to take someone else's identity are abuses.
- Misuse of the system is subject to discipline including discharge, or criminal prosecution depending on the severity of the violation.
- The city's possible tolerance of prior policy violations is no defense.

E. Monitoring

- All communication is subject to monitoring.

V. Internet

A. Use

- Internet use will be for city business purposes. Personal use of the internet connection shall be kept to an absolute minimum, and only during non-business hours. Internet activity is not private or confidential.
- Entertainment, games, sports and gambling, graphic or explicit materials are prohibited. Other “bypass” methods of access are not allowed.
- See Section IV. “D” Appropriate Usage.

VI. Remote Network Access

- Remote access to our city network via Virtual Private Network (VPN) Client will be provided to city employees, council members and contractors as authorized.
- Rights to access network resources will be controlled by network login and passwords.
- Remote access must use MFA to establish a connection to secure the credentials and further limit access for outside malicious users.
- All remote access users are subject to the rules and regulations set forth in this policy for all network users.

VII. Voice Mail

Usage of voice mail shall be governed under the same policies as email and Internet. Messages should not be considered “private”. The voice mail system retains new messages indefinitely. Messages which have been “archived” will remain in your mailbox for 30 days; however, we suggest that you delete messages as soon as possible to avoid storage capacity problems in the voicemail system.

VIII. Mobile Devices

If a mobile device will be non-city owned but used at least in part for city business and connect to city IT systems, then the user must read the Non-City Owned Mobile Device Acceptable Use policy and sign the agreement.

IX. IT Security Training

All users will participate in training as prescribed by the city and administered by IT.

IX. Affidavit

Prior to computer use, the user will sign an affidavit that states that they have received and read a copy of the city of New Hope Information policies statement.