CITY POLICIES REGARDING
GENERAL COMPUTER USE, DOCUMENT STORAGE,
E-MAIL AND INTERNET ACCESS

City of Berkley, Michigan
Adopted: February 16, 2007
Revised: July 2009

Contents

Introduction 2
General Computer Policies 2
Non-City Owned Devices 2
General E-Mail Procedures 3
  Viruses & E-Mail Attachments 3
Internet Use 4
  Instant Messaging & Peer to Peer File Sharing 4
Passwords *(revised 06/17/08)* 4
Document Storage 5
  Saving Personal Files 6
Laptop Security 6
  Preventing Laptop Theft 6
  Traveling With A Laptop 6
  Protecting Laptop Data 6

Introduction

The purpose of this policy is to define the proper use of e-mail and Internet services for the City of Berkley. All users of the City's computer systems are covered by this policy.

The City of Berkley is committed to providing an environment that encourages the use of computers and electronic information as essential tools to support the community. When communicating using the city's e-mail system and Internet connection, you are representing the City of Berkley. It is the responsibility of each employee to ensure that this technology is used for proper business purposes and in a manner that does not compromise the confidentiality of proprietary or other sensitive information.

General Computer Policies

- Only those persons employed by the City are permitted to use any computer resources owned, rented or leased by the City of Berkley. Exceptions may be made by the City Manager or IT Coordinator on a case by case basis.
- Only the IT Coordinator or designated representative may install software or hardware on any City computer. All other hardware or software installations are strictly prohibited unless specific permission has been granted by the City Manager. Designated representatives may include contract support staff.
- The City purchases and licenses the use of various software for business purposes and does not own the copyright to this software or related documentation. Installing unlicensed software (including exceeding the number of licenses purchased) is illegal and strictly prohibited.
- Downloading software is prohibited without express permission from the City Manager or IT Coordinator. If approved – explicit instructions must be followed in order to protect the computer and network from viruses and other types of malware.
- Any unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to: connecting to, posting, or downloading pornographic material; engaging in computer "hacking" and other related activities; attempting to disable or compromise the security of information contained on the City's computers.

Non-City Owned Devices

- Personal equipment – such as but not limited to – computers, laptops, printers, scanners, personal digital assistants, cameras, cell phones – may be not connected to a city device or Internet connection without the prior consent of the City Manager or IT Coordinator. Such devices shall first be checked for up to date virus software and scanned for viruses if appropriate.
- Likewise - employees shall not allow any non-employee, contractor, subcontractor or vendor to connect any such device to any city equipment or Internet connection without the prior consent of the City Manager or IT Coordinator. Such devices shall first be checked for up to date virus software and scanned for viruses if appropriate.

General E-Mail Procedures

- The City's e-mail program is provided for business-related purposes.
- All e-mail correspondence is the property of the City of Berkley. The Internet is not to be used to communicate personal views or to transmit offensive or libelous material.
- Employee e-mail communications are not considered private despite any such designation either by the sender or the recipient.
- E-mail messages should not be treated as confidential or secure. Anything sent through e-mail passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way.
- The City reserves the right to monitor its e-mail system - including an employee's mailbox - at its discretion in the ordinary course of business. Please note that in certain situations, the City of Berkley may be compelled to access and disclose messages sent over its e-mail system.
- The existence of passwords and "message delete" functions do not restrict or eliminate the City's ability or right to access electronic communications.
- Employees shall not share an e-mail password or provide e-mail access to an unauthorized user.
- Employees shall not post, display or make easily available any access information, including, but not limited to, passwords.
- Offensive, libelous, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the City's policies concerning equal employment opportunity, sexual Harassment or other unlawful harassment.

Viruses & E-Mail Attachments

- All e-mail attachments must be scanned for viruses before opening.
- Files stored on external media (cd, floppy, flash drive, etc), must be scanned before opening using up-to-date virus scanning software.
- Any questions about how to scan for viruses are to be directed to IT Coordinator.

Internet Use

- Postings placed on the Internet will display the City's domain name address, berkleymich.org. Hence, posting is allowed only if the message is work-related. For instance, Technical questions may be placed on a manufacturer's web site or bulletin board for them to respond to. Under no circumstances shall information of a confidential, sensitive or otherwise proprietary nature be placed on the Internet.

- Internet Service Providers (like WOW, Comcast, AOL, etc.) provide subscribers with free space to host their own web pages. No employee may create any type of web page that represents itself as an official City of Berkley website without permission from the City Manager.

- Subscriptions to news groups and mailing lists are permitted when the subscription is for work-related purposes. Any other subscriptions are prohibited.

- Information published on the Internet may be copyrighted. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the author or copyright holder.

Instant Messaging & Peer to Peer File Sharing

- Two technologies that have become popular on the Internet are Instant Messaging (IM) and Peer to Peer File Sharing (P2P). Both of the technologies are very insecure and if used, would expose our network and data to security threats. Use of these technologies is prohibited.

Passwords *(revised 06/17/08)*

- Must be a minimum of 7 characters
- Cannot contain your account name or parts of your full name that exceed two consecutive characters
- Must contain characters from three of the following four categories:
    - uppercase characters (A through Z)
    - lowercase characters (a through z)
    - numbers: 0 through 9
    - Special characters (for example, !, $, #, %)
- Passwords will expire every 120 days and must be reset.

Passwords are not to be shared with anyone. Each employee must use their own logon and password. Directors who need a list of employees who have network access should contact the IT Coordinator.

A good password is a combination of upper and lower case letters, numbers, special characters.

If employees' passwords must be written down, it should be kept in a secure location that no one else can find (not on a sticky note attached to the computer, under the keyboard, etc.)

Document Storage *(revised 07/29/09)*

My documents, My computer or Desktop
Documents saved to this location are:

- stored on your local drive only
- accessible only to the document author
- cannot be accessed by a coworker in the document author's absence
- not backed up
- will be irretrievably lost in the event of a hard drive failure or if your pc is replaced
- **DO NOT SAVE DOCUMENTS HERE UNLESS YOU ARE PREPARED TO LOSE THEM!**

External devices:
Examples of external devices include: USB flash drive, floppy disks, CDs, etc.
Documents saved to this location are:

- easy to lose
- easily damaged
- may be inaccessible to coworkers in an employee's absence
- not backed up
- **Saving documents to this location is not recommended**.

Department directory:
Your department directory has the name of your department in it – e.g. "communications on FS03"
Documents saved to this location are:

- accessible to coworkers when needed
- stored on the file server
- backed up nightly
- **This is the best place to save documents that need to be accessible to coworkers**.

Home directory:
Your home directory has your name in it - e.g. "bcole on FS03"
Documents saved to this location are:

- not accessible to coworkers when needed
- stored on the file server
- backed up nightly
- **This is the best place to save documents that are confidential and that will not be needed by coworkers in an employee's absence.**

City directory:
The City directory is named "city on FS03"
Documents saved to this location are:

- visible to anyone that can log in to the network
- stored on the file server
- backed up nightly

Saving Personal Files

Saving of personal files should be kept to a minimum. Photos, screen savers/wall paper take up considerable space on our servers and cause interruptions in our backup. Employees should limit themselves to no more than six photos. The server is routinely scanned for such files, when an excessive amount of such files are found they are deleted.

Laptop Security

Preventing Laptop Theft

- Laptop users will be provided with a security cable. Security cables are to be used at all locations (office, conference room, hotel rooms, etc). Report a missing laptop immediately to the IT Coordinator.

Traveling With A Laptop

- Laptops should not be left unattended for any length of time. Security cable should be used in places like hotel rooms, meeting rooms. Employees should do their best to keep an eye on laptops when going through security checkpoints.

- An ID, such as a nametag or business card should be taped to the top of your laptop.

- Laptops should never be with checked luggage and should be carried on board. Laptops should be charged for inspection by airport security staff.

Protecting Laptop Data

- Data stored on a laptop hard drive should be backed up frequently. Backups can be made to CDs or thumb drives.

- Laptops should not be set to save passwords or automatically log on to websites.

- Caution should be used with Wi-Fi access. With unencrypted Wi-Fi, every password, email message, and Web page can be read by any other user on that Wi-Fi network. If the security status is unknown e-mail and programs requiring the use of private information should not be used.