



ADMINISTRATIVE INSTRUCTION NO. 8 CITY OF BOWLING GREEN

COMPUTER USE POLICY

1.0 Overview

The City of Bowling Green's intentions for publishing an Acceptable Use Policy are to provide a framework for proper and safe use of the City's computer network and in doing so protect employees, partners and the organization.

Information systems, including but not limited to computers, servers, switches, software, CDs, USB drives, PDAs, network accounts, email accounts, fax machines, printers are the property of the City of Bowling Green. These systems are to be used for business purposes in serving the interests of the citizens of Bowling Green.

Effective computer security is a team effort involving the participation and support of every City of Bowling Green employee and affiliate who deals with information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

While the City of Bowling Green's Administration desires to provide a reasonable level of privacy, employees should be aware that the data they create on the organization's systems remains the property of the City of Bowling Green.

The Information Technology (IT) Manager and IT staff, under the general direction of the Municipal Administrator, or his designee, are charged with managing and maintaining information systems within the City of Bowling Green organization.

Only persons who have signed this policy and thereby agreed to follow it will be permitted to connect to log on to or use any City of Bowling Green owned or leased information asset or network.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computers and the network at the City of Bowling Green. These rules are in place to protect the employee and the City of Bowling Green organization. Inappropriate use exposes the City of Bowling Green network to risks including virus attacks, data theft, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants and temporaries at the City of Bowling Green, including all personnel affiliated with third parties.

1. Exception:

- a. The City of Bowling Green, Municipal Utility SCADA networks, which will remain isolated from all other networks, including the Internet, is exempt from this policy and will be managed and maintained through a separate policy.

4.0 Policy

4.1 Electronic Business Records

Business related email messages and other electronic documents are considered business records of the City. Accordingly, they are public information which may be used in administrative, judicial, or other proceedings. Furthermore, their destruction must be done within the parameters established for the destruction of public records. Once a message or document has been saved in hardcopy format, it may be deleted from the computer's hard-drive.

Personal email messages and electronic documents are not deemed to be business records, are not considered a public record and as such are not subject to the Public Records Law of the State of Ohio.

4.2 General Computer Use

1. Employees will cooperate fully with requests made by IT staff with regard to information systems owned or leased by the City of Bowling Green.
2. Only software licensed to the City of Bowling Green shall be used on City of Bowling Green owned or leased computer hardware.
3. The original copy of all software licenses will be kept and secured by the IT.
4. Employees may install Windows/Office automatic updates and software accessed via the "Control Panel"/"Add or Remove Programs"/"Add New Programs" button. All other programs will be installed by IT staff.
5. Unauthorized software will be removed immediately and the individual who was logged on when the software was installed will be reported to the Personnel Director for disciplinary action.
6. Select categories of web sites are blocked from access (e.g. games, webmail, gambling, personal web pages and pornography). If you find that a legitimate business related web site is blocked, you can contact IT and have the block removed.
7. The use of default Windows or other games is not permitted on City computers.
8. Excessive personal use of the Internet may lead to discipline. Employees are responsible for exercising good judgment regarding reasonable personal internet use. If there is any uncertainty, employees should consult their supervisor, manager or IT staff.
9. The email system, like all City property, is to be used to conduct City business. Sending and receiving personal email messages are allowed, but will be kept to a minimum.
10. Employees can modify their desktop wallpaper and screen saver to their liking provided it isn't harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.
11. IT Division may monitor and audit equipment, systems and network traffic to ensure compliance with this policy. Specific auditing of electronic messaging will require the authorization of the Municipal Administrator.

4.3 General Network and Computer Security

1. Error messages, unusual computer activity and suspected network security breaches will be brought to the attention of IT staff IMMEDIATELY.
2. Information displayed on computer screens should be considered confidential. Employees will take all necessary steps to prevent unauthorized access to this information.
3. Sharing any information about the nature or setup of the City's computer network with anyone is strictly prohibited. All such inquiries will be directed to IT staff.
4. IT will be notified immediately when a portable computer, Blackberry, USB drives or storage device is lost or stolen so that passwords can be changed and other security and damage control measures taken.
5. Only the person logged onto the computer may use it at that time.
6. You are responsible for everything that occurs during your session. If sharing a computer, be sure to log off before another person uses it.
7. iSeries (AS 400) and Windows passwords will be changed at least quarterly (every 90 days).
8. Windows passwords will be a minimum of six characters in length, will not be dictionary words or proper names and will utilize at least three of the following:

- a. Upper case letters (A-Z)
 - b. Lower case letters (a-z)
 - c. Numbers
 - d. Special characters (e.g. #, %, &, @, /, \, ^, etc...)
9. Password security is typically the weakest link in information systems security, therefore:
- a. Don't reveal your password to ANYONE, EVER!
 - b. Don't hint at the format of a password (e.g., "my address").
 - c. Don't share your password with family members or friends.
 - d. Don't display your password in any manner.
 - e. If you forget your password, IT staff will reset it for you.
 - f. If you need access to someone's data who is not available, let your supervisor know and he/she can ask IT staff to grant you access.
10. Users should log-off when the computer will be unattended (Windows key + "L" for Windows XP users or Control-Alt-Delete for Windows 2000 and Windows XP users).
11. City owned laptops should never be left unsecured or unattended in public places. Sensitive data will be stored in encrypted files, folders or drives.
12. Every computer used by an employee, vendor or contractor that is connected to the City of Bowling Green network shall be continually executing virus-scanning software with a current virus data file.
13. Computer users must use extreme caution when opening email attachments received from unknown senders. Normally, the best course of action is to simply delete the emails from unknown sources.
14. Any email attachment received from outside our network may contain viruses and will be scanned with an up to date anti-virus program prior to opening.
15. Access into the network from the Internet will only occur via encrypted VPN tunnels set up by IT staff.
16. All data connections within the City's network will be set up, monitored and maintained by IT staff. This includes wireless, Wi-Fi, Bluetooth, cellular, WiMAX, etc...

4.4 Unacceptable Use

Under no circumstances is an employee of City of Bowling Green authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City of Bowling Green owned resources.

Unacceptable Network and Computer Activities

The following activities are strictly prohibited:

1. Using a City of Bowling Green computing asset to conduct business for other agencies or companies or for themselves.
2. Connecting any PC, laptop, server, wireless device, PDA, cell phone, printer, camera, switch, router or monitoring device to the network without the explicit approval of IT staff.
3. Logging into a server, folder or account that the employee is not expressly authorized to access.
4. Circumventing user authentication or security of any computer, network or account.
5. Unauthorized use of or the illegal copying of copyrighted material including, but not limited to, photographs, books, music, video or software.
6. Modifying any computing or networking hardware whether owned or leased by the City of Bowling Green. (e.g. adding or removing a CD ROM Drive or modem)
7. Blocking IT staff's access to a computer or networking device. (e.g. Setting up a BIOS password or unplugging a network cable)
8. Use of any form of network monitoring which will intercept data not intended for the employee.
9. Viewing, sending, forwarding, downloading, or searching for obscene, pornographic, or illegal material.
10. Use of internet streaming media, whether audio or video, for entertainment. This includes, but is not limited to internet radio, internet TV and internet movies.
11. Use of any P2P (Peer to Peer) or Bit-Torrent file sharing.

Email and Communications Activities

1. Unless specifically authorized to do so, employees are prohibited from using email to transmit confidential information to outside parties. Confidential information includes but is not limited to customer lists, credit card numbers, Social Security numbers, employee performance reviews, salary details, passwords, and information that could embarrass the City of Bowling Green and employees were it to be made public.
2. Any form of harassment via email, whether through language, frequency, or size of messages.
3. Forwarding or sending "chain letters" or other "pyramid" schemes of any type.
4. Sending email as someone other than yourself, without the other person's approval (e.g. using "send on behalf of"), or sending anonymous email.
5. Use of any form of webmail (other than BGOHIO.ORG webmail).
6. Use of any form of Instant Messaging (Twitter, AIM, Yahoo IM, IRC, Gmail Chat, etc...) except for business use as approved by the Municipal Administrator.
7. Use of any forms of Voice over IP (VoIP) such as Skype except for business use.

Law Enforcement personnel are exempt from Section 4.4 during the performance of specially assigned duties. (e.g. tracking child predators or investigating criminal activity)

4.5 Removable Media Use

Removable media is a well-known source of viruses and has been directly tied to the loss of sensitive information in many organizations. Examples of Removable Media include floppy disks, CDs, DVDs, thumb drives and other USB and Firewire drives.

1. City of Bowling Green staff may only use City of Bowling Green owned removable media in their work computers.
2. Before inserting removable media into a City computer, the user will insure that the computer is running the most recent anti-virus update available.
3. When sensitive information is stored on removable media, it must be encrypted.

4.6 Solicitation

City email accounts shall not be used to solicit for non-City related business ventures, personal parties, social meetings, union meetings, charities, political causes, religious causes, or other matters not connected to the City's operation.

Employees may use City e-mail accounts for solicitation for charitable organizations with prior approval by the Municipal Administrator or his/her designee. Furthermore, such solicitation will be permitted based on whether or not the charitable organization(s) are true health and welfare charities. The City of Bowling Green will not permit the solicitation for organizations whose main purposes are to attempt to influence elections and/or to influence public policy.

5.0 Enforcement

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

6.0 Revision History


John B. Quinn
Mayor

4-22-09
Date