# CITY OF MARSHFIELD
# INFORMATION TECHNOLOGY POLICY 8.010 - TECHNOLOGY USE AND ACCESS

| Section | Title | Page |
|---|---|---|

# CITY OF MARSHFIELD TECHNOLOGY USE AND ACCESS POLICY

## I. GENERAL

The City of Marshfield (hereafter referred to as City) provides employees with electronic access and the means to do so, consisting of electronic communication systems, a network connection, and Internet/intranet access. This policy governs all use of the City's network, Internet/intranet, electronic communications-related systems access and all associated technology at all City locations and offices. This policy includes, but is not limited to, computer equipment, telecommunications equipment, software, operating systems, storage media, and network accounts providing electronic-mail, Internet, FTP (File Transfer Protocol), chat, news groups, electronic bulletin boards, the City's intranet and all other City electronic messaging and communications systems.

### A. Purpose

The purpose of this policy is to outline the acceptable use of technology at the City. These rules are in place to protect employees and the City. Inappropriate use exposes the City and its users to risks including virus attacks, compromise of network systems and services, privacy/confidentiality breech, potential interruption of services (including emergency and protective services), and legal issues including excess and unforeseen liability.

### B. Scope

This policy applies to all City employees, elected officials, Commissioners, Committee/Board members, customers, visitors, guests, external contractors/vendors, consultants, all personnel affiliated with third parties, or anyone else when they are using equipment or systems that are owned or leased by the City, whether during or outside of work hours.

### C. Use and Ownership

Use of City technology is a privilege, not a right. Use of the network, associated systems, and Internet/intranet access extends throughout an employee's term of employment, providing the employee does not violate the City's policies regarding network, Internet/intranet, and electronic communications use. Any person not actively under the City's employ or assign does not have permission to access or use any City system or devices unless said device is specifically designated for "public" or "guest" use by the Information Technology Department.

The City's communications systems, network, and Internet/intranet access are intended for business use only. The City does, however, identify the work-place environment and employee convenience value of personal use of these systems. Therefore, incidental, non-disruptive, casual personal use may be tolerated at the <u>sole</u> discretion of supervisors or managers and the Information Technology Department head. Such use is tolerated providing it does not interfere with the performance of duties and/or the business use of these systems, represents a marginal aggregate use, and is in strict compliance with all other terms of this and all other current and future City policies.
--**If there is any uncertainty regarding permissible personal use, it is the responsibility of the employee to consult his or her supervisor or manager for clarification before proceeding**.--

**All information created, transmitted, or received via the City's electronic infrastructure, including but not limited to, e-mail system, network, or Internet/intranet, including all e-mail messages and electronic files, is the property of the City. Employees should have no expectation of privacy regarding this information. The City reserves the right to access, read, review, monitor, and copy all messages and files on its computer system at any time and without notice. Employees should be aware that any content created or transmitted via these systems may constitute Open or Public Record and therefore may be subject to public disclosure in accordance with Local, State and Federal laws. When deemed necessary, the City reserves the right to disclose any electronic records or data to law enforcement agencies, the media, or other third parties without the employee's consent.

## II. ELECTRONIC COMMUNICATIONS

### A. Policies and Procedures

The City's electronic communications systems are designed to improve service to our customers and citizens, enhance internal communications, reduce service provision costs, and reduce paperwork. Employees using the City's e-mail, voicemail, and all associated systems must adhere to the following policies and procedures:

- Personal e-mail accounts are not permitted unless for City business purposes and expressly authorized in advance by the Information Technology Department head. Such accounts will be set up and configured exclusively by City Information Technology Department staff.

- Alternate Internet Service Provider or Virtual Private Network connections to the City's internal network are not permitted unless expressly authorized by the Information Technology Department head and properly protected by a firewall or other appropriate security device(s) and/or software.

- Forwarding of external personal accounts inward or City e-mail accounts outward to a personal mail account is not permitted.

- Only authorized management personnel are permitted to access another person's e-mail or voicemail without the user's consent. Such access will only be granted by the Information Technology Department head with the permission of the Human Resources Manager or City Administrator.

- Employees should archive electronic communications (whether e-mail or voicemail) to prevent them from being automatically deleted. All messages archived in the City's computer system shall be deemed City property, as is all information on the City's systems. Employees are responsible for knowing, and complying with the City's electronic and public records retention policies.

## B. Protocol

- Use extreme caution to ensure that the correct e-mail address is used for the intended recipient(s).

- Any message or file transmitted must have the sending employee's name and pertinent contact information attached and must have a suitable subject line.

- All communications originating from or transmitted via the City must contain professional and appropriate language at all times. Employees are prohibited from transmitting abusive, harassing, intimidating, threatening, and discriminatory or otherwise offensive messages (whether through language, frequency, or size of messages) via e-mail, telecommunications, or paging. Sending such content will result in disciplinary action, up to and including termination, and may be subject to additional criminal and legal prosecution.

## C. Abuse

- All electronic communications must conform to existing and future City anti-harassment, workplace violence, and discrimination policies.

- Use of the City's electronic communications systems to solicit for any purpose, personal or otherwise, without the consent of the City is strictly prohibited. Although, as indicated in its Mission Statement, the City supports charitable and non-profit organizations, no City resources should be used to further these altruistic efforts without prior written authorization by department supervisors or managers, the knowledge of the Information Technology Department head, and with the concurrence of the City Administrator.

- Chain messages, "Ponzi," pyramid schemes, or programs should not reside on any City system and must be deleted immediately. Creating or forwarding any such content is prohibited. Any employee engaging in the transmission of inappropriate content, as determined by management, will be subject to disciplinary action, up to and including termination, as well as potential additional criminal and legal prosecution.

- Sending, forwarding, or hosting unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail SPAM) is prohibited. Posting non-business-related messages to large numbers of Usenet newsgroups (newsgroup SPAM) is prohibited. Engaging in such activity will result in disciplinary action, up to and including termination, and may be subject to additional criminal and legal prosecution.

- Unauthorized use, forging, or altering of e-mail header information is prohibited. Falsifying or altering any electronic transmission will result in disciplinary action, up to and including termination and may be subject to additional criminal and legal prosecution.

### D. Confidentiality/Privacy

- At this time the City does not have the resources to adequately and effectively encrypt e-mail communications. Consequently, sensitive, confidential, or vulnerable information should never be sent via e-mail. This includes, but is not limited to, the transmission of customer/citizen financial information, Social Security numbers, employee health records, and other confidential material.

- Employees should exercise sound judgment when distributing messages. Customer/citizen-related messages should be carefully guarded and protected. Employees must also abide by copyright laws, ethics rules, and other applicable current and future City policies or laws.

## III. NETWORK AND INTERNET

### A. Personal Responsibility

Effective security, availability, integrity, and protection of systems is a team effort involving the participation and support of every City employee and affiliate who deals with information technology and/or information technology systems. It is the responsibility of every computer user to know these guidelines, and to conduct his or her activity accordingly. By accepting an account, related credentials, and accessing the City's network, Internet/intranet, or other communications system, an employee agrees to adhere to the City policies regarding their use. Every user also agrees to report any misuse or policy violation(s) to his or her supervisor or the City's Information Technology Department head **in a timely manner**.

### B. Availability and Access

The City reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violations, security, or other concerns.

### C. Content and Communications

The City, at its sole discretion, will determine what materials, files, information, software, communications, and other content and/or activity will be permitted.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Likewise, it is also relatively easy to spoof another user on the Internet; contacts made over the Internet should not be trusted until their identity can be confirmed via alternate means. Wiretapping and message interception are straightforward and frequently encountered on the Internet. The validity and authenticity of any content or communication obtained from the Internet is the sole responsibility of the user.

### D. Privacy

*Network and Internet access is provided as a tool for City business and to serve the interests of the City, its customers and citizens in the course of normal business. The City reserves the right to monitor, inspect, copy, review, and store at any time,

without prior notice, any and all usage of the network and the Internet/intranet, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of the City. An employee should have **no expectation of privacy** regarding any systems or the use of said systems. Network administrators may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring employees are using the system consistently with City policy.

## E. Security

The integrity and protection of City electronic resources is the responsibility of each person who utilizes the system. Any user's activity can be the weakest link of the entire City enterprise and infrastructure. Users are our first means of accountability and physical security, therefore each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.

2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that others may know them. Passwords should not be recorded where they might be easily obtained.

3. Will change passwords at least every 90 days.

4. Should use passwords that will not be easily guessed by others.

5. Should log out or lock their workstation when away from it.

6. Should store storage media and devices out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.

7. Should keep storage media and devices away from environmental hazards such as heat, direct sunlight, and magnetic fields.

8. Must protect critical computer equipment, e.g., file servers, by an uninterruptible power supply (UPS). A surge suppressor should protect other computer equipment.

9. Should avoid exposing hardware and devices to environmental hazards such as food, smoke, liquids, high or low humidity, and extreme heat or cold.

10. Should not perform installations, disconnections, modifications, and relocations to any equipment since the Information Technology Department is responsible for these activities. This does not apply to temporary moves of portable equipment.

11. Shall not take shared portable equipment such as laptop computers off site without the informed consent of the Information Technology Department. Informed consent means that Information Technology personnel know what

equipment is leaving, what data is on it, and for what purpose it will be used.

12. Should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

13. Should UNDER NO CIRCUMSTANCES connect ANY outside equipment to ANY City system, without exception. Foreign devices have the unique ability to circumvent all security and protections in place at the City. Any employee noticing another employee or individual connecting unknown equipment should immediately alert the Information Technology Department.

## F. Viruses and Malicious Programs

It is the responsibility of everyone who uses the City's computer network and all associated systems to take reasonable measures to protect our assets from virus infections. Computer viruses are much easier to prevent than to cure. There are actually three various types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. When an infected file is opened from a computer connected to the City's network, the virus can spread throughout the network and may do damage. A Trojan horse is an actual program file that, once executed, doesn't spread but can damage the computer on which the file was run. A worm is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run.

### 1. Introduction

Viruses can enter the City's systems in a variety of ways:

a. **E-mail—**By far, most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect the City's network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.

b. **Disk, CD, Zip disk, or other media—**Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.

c. **Software downloaded from the Internet—**Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.

d. **Instant messaging attachments—**Although less common than e-mail attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as e-mail viruses, but they are transmitted via instant messaging software.

## 2. Prevention and /or Minimization of Damage

The Information Technology Department fights viruses in several ways:

a. **Scanning Internet traffic—**All Internet traffic coming to and going from our network must pass through company servers and other network devices. Only specific types of network traffic are allowed beyond the organization's exterior firewalls.

b. **Running server and workstation anti-virus software—**All vulnerable servers run anti-virus scanning software. This software scans our file data stores ("F:\" or "N:\" drive), looking for suspicious code.

   Protection software is also installed on all City workstations and mobile devices. This software scans all data written to or read from a unit's hard drive. If it finds something suspicious, it isolates the dubious file, forwards it to our anti-virus quarantine, and automatically notifies the Information Technology Department.

c. **Routinely updating virus definitions—**Every day, the server virus scanning programs check for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated.

   On a continuous basis, the workstation virus protection program checks with the anti-virus server on the network for updates. The workstation program will then download and install the update automatically, if one exists.

## 3. Response

Even though all Internet traffic is scanned for viruses and all files on the servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee's workstation, and if not properly handled, it could infect the City's systems.

**The IT staff will attempt to notify all users of credible virus threats via e-mail or the intranet. Because this notification will automatically go to everyone in the organization, employees should not forward virus warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic.**

As stated, it is the responsibility of all CityNet users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

- Do not open **unexpected** e-mail attachments, even from trusted senders.

- Never open an e-mail or instant messaging attachment from an unknown or suspicious source.

- Never download freeware, shareware, or any other files from the Internet.
- If a file you receive contains macros that you are unsure about, disable the macros.

### G. Downloaded Files

Files are not to be downloaded from the Internet without the prior **written** authorization of the Information Technology Department. Any files authorized for download from the Internet must be scanned with virus detection software before being opened. Employees are reminded that information obtained from the Internet is not always reliable and should be verified for accuracy before use. Content authorized to be downloaded from an untrusted or unknown provider must be tested by the Information Technology Department on a stand-alone (not connected to the network), nonproduction machine.

### H. Confidential Information

Employees may have access to confidential information about the City, other employees and customers or citizens. Within the bounds of assigned job duties and with the approval of management, employees may use electronic communications to transmit confidential information **internally** to those with a legitimate business need to know. Such communications must always be designated as "Confidential." The official record custodian will make the determination of confidentiality. For purposes of this policy, confidential information includes, but is not limited to:

1. Procedures for computer access and sign-ons to the City's, clients' or vendors' systems; program manuals, user manuals, or other documentation; screen, file, or database layouts; systems flowcharts; and all documentation normally related to the design or implementation of any system developed by the City relating to computer programs or systems installed either for customers, citizens, or internal use;

2. Lists of present employees, clients, and customers and the names of individuals with whom the City deals, the type of equipment or computer software they use, and information relating to those clients and customers, which has been given to the City by them or developed by the City, relating to computer programs or systems installed;

3. Lists of, or information about, persons seeking employment with or who are employed by the City;

4. Any other information relating to the City's infrastructure, engineering, or utilities.

## IV. SOFTWARE USAGE

### A. Policies and Procedures

Software piracy is both a crime and a violation of the City's Software Usage Policy.

Employees are to use software strictly and exclusively in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (except for backup and archival purposes by designated Information Technology personnel) is a violation of copyright law. In addition to being in violation of the law, unauthorized duplication of software is contrary to the City's standards of employee conduct.

To ensure compliance with software license agreements and the City's Software Usage Policy:

1. Employees must use software in accordance with the manufacturer's license agreements and the City's Software Usage Policy. The City licenses the use of computer software from a variety of outside companies. The City does not own the copyright to software licensed from other companies. Employees acknowledge they do not own software or its related documentation. Employees may not make additional copies of software. The only exception will be a single copy, as authorized and deemed necessary by designated Information Technology personnel, for backup or archival purposes.

2. The City does not condone, and prohibits, the unauthorized duplication of software. Employees illegally reproducing software will be subject to disciplinary action, up to and including termination. In addition, employees illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment.

   **NOTE: Unauthorized reproduction of software is a federal offense under U.S. copyright laws. In the United States, violators may be subject to civil damages in amounts up to $150,000 per title copied. Criminal penalties include fines as high as $250,000 per software title copied, and imprisonment of up to 5 years.**

3. Any employee who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to the City shall be subject to disciplinary action, up to and including termination.

4. Any employee who places or uses unauthorized software on the City's premises or equipment shall be subject to disciplinary action, up to and including termination.

5. Under no circumstances are employees permitted to install their personal software onto the City's computer system. Employees are not permitted to copy software from the City's computer system for installation on home or other computers.

6. In cases that require an employee to use software at home, the City will purchase an additional copy or license or obtain the necessary authorization from the software publisher. Any employee issued additional copy(s) of software for home use acknowledges that such additional copy(s) or license(s) purchased for home use are the property of the City.

7. Employees are prohibited from giving software to persons not in the employ of the City. Under no circumstances will the City use software from an unauthorized source, including, but not limited to, the Internet, home, friends, and/or colleagues.

8. Employees who suspect or become aware of software misuse are required to notify their supervisor, manager, the Information Technology Department, or the Human Resources Manager.

9. All software used on City-owned computers will be purchased through appropriate procedures. Consult your supervisor, manager, or the Information Technology Department for proper procedures.

## V. COMPUTER EQUIPMENT

The following policies are designed to reduce repair costs, maintain the integrity of our system and protect the City's assets. Employees should adhere to the following:

- Do not keep liquids or magnets on or near the computer/workstation.

- Do not remove any computer or electronic device from the building unless the unit is specifically designated as a "check-out" or a mobile unit and proper notification has been given to the Information Technology Department.

- Do not transport media off site. This will help minimize exposure to viruses as well as preserve the confidentiality and privacy of City data.

## VI. COMPLIANCE

Although each individual is responsible for his/her own actions, management personnel are responsible for ensuring employee compliance with City policy.

Any employee aware of a policy violation should immediately report the violation to his/her supervisor, manager, the City's Information Technology Department and/or the Human Resources Manager.

For security and network maintenance purposes, authorized individuals within the City may monitor equipment, systems and network traffic at any time. The City of Marshfield reserves the right to audit networks and systems on a periodic basis to ensure compliance with City policy.

## VII. NONCOMPLIANCE

Employees who violate this policy and/or use the City's e-mail system, voicemail system, network, Internet/intranet, or any other technology systems or access for improper purposes will be subject to disciplinary action, up to and including termination.

**Any user having <u>personal</u> knowledge of misuse or violation(s) of this policy who fails to report such violation to his or her supervisor or the City's Information**

**Technology Department in a timely manner will be subject to disciplinary action, up to and including termination**.

## VIII. PROHIBITED ACTIVITIES

Employees are expressly prohibited from using the City's electronic communications systems, network, or Internet/intranet access for the following activities:

- Downloading software without the prior approval of the City's Information Technology Department.

- Unauthorized copying or printing of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City does not have an active license.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City.

- Using any software that is not licensed by the manufacturer **and** approved by the City Information Technology Department.

- Sending, exporting, printing, or otherwise disseminating confidential data or any other information deemed confidential or proprietary by the City, to unauthorized persons.

- Operating a business, soliciting money for personal gain, or otherwise engaging in commercial activity outside the scope of employment.

- Searching for or engaging in any activities soliciting outside employment.

- Making offensive or harassing statements based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.

- Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements. An employee should notify their supervisor and/or Human Resource manager immediately upon receiving such a message. This type of message should not be forwarded.

- Sending or forwarding a message that discloses personal information without City authorization. This shall also include accessing, transmitting, receiving, or seeking confidential information about clients or fellow employees without authorization.

- Sending ethnic, sexual-preference, or gender-related slurs and/or jokes via e-mail. “Jokes,” which often contain objectionable material, are easily misconstrued when communicated electronically.

- Sending or soliciting sexually oriented messages or images.

- Attempting to access or visit sites containing, or having electronic possession of, pornography, terrorism, espionage, theft, or drugs. In the event that such activity or content is necessary for the effective performance of assigned duties (protective services), prior written authorization must be obtained from a supervisor or manager AND the Information Technology Department head. Such written authorization will be maintained on-file in the Information Technology Department.

- Gambling or engaging in any other criminal activity in violation of City policy, or local, state, or federal law.

- Engaging in unethical activities or content.

- Participating in activities, including the preparation or dissemination of content, which could damage the City's professional image, reputation, and/or financial stability.

- Revealing your account password to others or allowing use of your account by others. Permitting or granting use of an e-mail or system account to another employee or persons outside the City. Permitting another person to use an account or password to access the network or the Internet/intranet, including, but not limited to, someone whose access has been denied or terminated, is a violation of this policy.

- Using another employee's password or impersonating another person while communicating or accessing the network or Internet/intranet.

- Introducing a virus, worm, Trojan, harmful component, corrupted data, unauthorized program, or the tampering in any manner with any of the City's computer systems or infrastructure.

- Effecting direct or indirect security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.

- Unauthorized port scanning or security scanning.

- Executing any form of network monitoring that will intercept data not intended for the employee or the employee's host, unless this activity is a part of the employee's normal job/duty **and** the Information Technology Department has been made aware of this activity.

- Circumventing user authentication or security of any host, network, or account.

- Interfering with or denying service to any user (for example, denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session or access, via any means, locally or via the Internet/intranet.

## IX. TECHNOLOGY USE AND ACCESS POLICY

**Acknowledgement of Receipt and Understanding**

I hereby certify that I have read and fully understand the contents of the Technology Use and Access Policy consisting of fifteen (15) pages including this page. Furthermore, I have been given the opportunity to discuss any information contained therein or any concerns that I may have. I understand that my employment and continued employment is based in part upon my willingness to abide by and follow the City's policies, rules, regulations and procedures.

I acknowledge that the City reserves the right to modify or amend its policies at any time, without prior notice. These policies do not create any promises or contractual obligations between this City and its employees. My signature below certifies my knowledge, acceptance and adherence to the City's policies, rules, regulations and procedures regarding Electronic Access.

Signature _____ Date _____

Print Name _____