

6-TECHNOLOGY ACCEPTABLE USE POLICY

Introduction

Computer information systems and networks are an integral part of business at the City of Waynesboro. The City has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

- Protect the City's investment,
- Safeguard the information contained within these systems,
- Reduce business and legal risk, and
- Protect the good name of the City.

Violations

Violations of this policy are a serious offense and will result in disciplinary action in accordance with City of Waynesboro 1996 employee handbook, as amended. Disciplinary actions may range from access privileges being withdrawn up to and including termination or even legal action depending upon the type and severity of the violation, whether it causes any liability or loss to the City, and/or the presence of any repeated violation(s).

Administration

The Information Technology department is responsible for the administration of this policy.

Scope

These policies apply to all employees, contractors, consultants, temporaries and other users. Throughout this policy, the term employee will be used to collectively refer to all such individuals. The policy also applies to all computer and devices connected to the City network. Communications resources include servers, networking facilities, e-mail system, workstations, software, video and telephone systems.

Contents

The topics covered in this document include:

- Statement of responsibility
- The Internet and e-mail
- Computer viruses
- Access codes and passwords
- Physical security
- Copyrights and license agreement

TECHNOLOGY ACCEPTABLE USE POLICY (cont'd)

Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

Manager responsibilities

1. Ensure that all appropriate personnel are aware of and comply with this policy.
2. Create control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

IT responsibilities

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Monitor compliance with Internet security requirements, including hardware, software, and data safeguards.
3. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

Internet and e-mail

The use of the Internet is a privilege, not a right. The purpose of this policy is to establish procedures and requirements to define appropriate uses and ensure the appropriate protection of City information and resources.

Policy

Access to the Internet is provided to employees for the benefit of the City and its citizens. To ensure that all employees are responsible and productive Internet users and to protect the City interests the following guidelines have been established for using the Internet and e-mail. The City encourages the business use of electronic communications as a productivity enhancement tool.

Acceptable use

Employees using the Internet are representing the City. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Acceptable uses include:

Using Web browsers to obtain business information from Web sites.

Accessing databases for information as needed.

Using e-mail for business contacts.

Incidental personal use is permissible as long as it does not interfere with staff productivity and does not preempt any business activities.

Employees may use the Internet for non-business research or browsing outside of normal working hours provided that all other usage policies are adhered to.

TECHNOLOGY ACCEPTABLE USE POLICY (cont'd)

Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the City, or nonproductive. Examples of unacceptable use are:

Interfering with the activities of others or use a disproportionate share of resources.

Send messages only to those who may be interested in the content. Examples of inappropriate use of resources are shown below. These actions frequently result in complaints and subsequent disciplinary action.

Sending or forwarding chain e-mail (i.e., messages containing instructions to forward the message to others) and broadcasting e-mail (i.e., sending the same message to more than 10 recipients or more than one distribution list)

Conducting a personal business using City resources.

Transmitting any content that is offensive, harassing, or fraudulent.

The Internet may not be used for illegal or unlawful purposes including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, forgery and computer tampering.

Downloads

File downloads from the Internet are not to be stored or installed on City computers unless specifically authorized by the IT department.

Employee responsibilities

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet.
3. Do not transmit copyrighted materials without permission.
4. Know and abide by all applicable City policies dealing with security and confidentiality of records.
5. Run a virus scan on any executable file(s) received through the Internet.
6. Avoid transmission of nonpublic information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.
7. Chats and newsgroups are public forums. If views or opinions are openly expressed in these forums, it should be clearly stated that these are personal and do not necessarily represent the views and opinions of the City.
8. Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the City and/or legal action by the copyright owner.

TECHNOLOGY ACCEPTABLE USE POLICY (cont'd)

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the City and *may be regarded as public information*. The City reserves the right to access the contents of any messages sent over its facilities if the City believes, in its sole judgment, that it has a business need to do so.

IT maintains systems in place to monitor and record Internet usage. The security systems are capable of recording each Web site visited, each chat, newsgroup or email message, and each file transfer into and out of the network. These security logs may be distributed to department directors.

It is the policy of the City NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications system monitored to support operational, maintenance, auditing, security and investigative activities.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. **This means don't put anything into your e-mail messages or visit internet sites that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

Computer viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources. Computer viruses are much easier to prevent than to cure. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

IT responsibilities

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee responsibilities

1. Employees shall not knowingly introduce a computer virus into City computers.
2. Employees shall not load diskettes of unknown origin.
3. Incoming diskettes shall be scanned for viruses before they are read.
4. Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and notify the IT department.

TECHNOLOGY ACCEPTABLE USE POLICY (cont'd)

Access codes and passwords

The confidentiality and integrity of data stored on City computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user unless there is department need. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

IT responsibilities

The IT department shall be responsible for the administration of access controls to all City computer systems. IT will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor. Deletions may be processed by an oral request prior to reception of the written request.

Employee responsibilities

1. Any employee who attempts to disable, defeat or circumvent a City security facility will be subject to immediate disciplinary action.
2. Shall be responsible for all computer transactions that are made with his/her user account and password.
3. Employees should not use accounts and passwords they are not authorized to use.
4. Shall not disclose passwords to others, unless there is a department need. Passwords must be changed immediately if it is suspected that they may have become known to others without the knowledge of the user. Passwords should not be recorded where they may be easily obtained.
5. Will change passwords at least every 180 days.
6. Use passwords that will not be easily guessed by others.
7. Log out or use a password-protected screen saver when leaving a workstation for an extended period.

Supervisor's responsibility

Managers and supervisors should notify IT promptly, in writing, whenever an employee leaves the City or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Human resources responsibility

The Human Resources Dept will notify IT of associate transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

TECHNOLOGY ACCEPTABLE USE POLICY (cont'd)

Physical security

It is City policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

IT responsibilities

1. The IT department is responsible for all equipment installations, disconnections, modifications, and relocations.
2. Ensure hardware purchased by the City is identified for asset tracking purposes according to City policy.

Employee responsibilities

1. Diskettes should be stored out of sight when not in use. Diskettes should not be used to store highly sensitive or confidential data.
2. Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment (e.g. file servers) must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Employees are not to perform equipment installations, disconnections, modifications, and relocations. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT.
6. Employees should not attach or install hardware to systems that has not been approved by IT.
7. Employees shall not take shared portable equipment such as laptop computers out of the office without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
8. Employees 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.
9. Employees must not establish dial-up access via modem to or from any workstation to create Internet connections.

TECHNOLOGY ACCEPTABLE USE POLICY (cont'd)

Copyrights and license agreements

It is the City's policy to comply with all laws regarding intellectual property. In doing so, one must use only legal versions of copyrighted software in compliance with vendor licensing requirements. This directive applies to all software that is owned by the City, licensed to the City, installed on City computers, or developed using City resources by employees or vendors.

Legal reference

The City and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose the City and the responsible employee(s) to civil and/or criminal penalties.

IT responsibilities

1. Maintain records of all software licenses owned or leased by the City.
2. Annual software audits to verify that only authorized software is installed.
3. Install software in a manner consistent to licensing agreements.

Employee responsibilities

1. Do not install software unless authorized by IT. Only software that is licensed to or owned by the City is to be installed on City computers.
2. Prohibited from downloading or copying software unless authorized by IT.

Civil penalties

Violations of copyright law expose the City and the responsible employee(s) to the following civil penalties:

Liability for damages suffered by the copyright owner
Profits that are attributable to the copying
Fines up to \$100,000 for each illegal copy

Criminal penalties

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b))," expose the City and the employee(s) responsible to the following criminal penalties:

Fines up to \$250,000 for each illegal copy
Jail terms of up to five years

Acknowledgment of Information Security Policy

This form is used to acknowledge receipt of, and compliance with, the City of Waynesboro Information Security Policy.

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return this page only to the information services manager.

Signature

By signing below, I agree to the following terms:

- i. I have received and read a copy of the "Information Security Policy" and understand the same and comply with;
- ii. I understand and agree that any computers, software, and storage media provided to me by the City contains proprietary and confidential information about City of Waynesboro and its customers or its vendors, and that this is and remains the property of the City at all times;
- iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at City of Waynesboro), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
- iv. I agree that, if I leave City of Waynesboro for any reason, I shall immediately return to the City the original and copies of any and all software, computer materials, or computer equipment that I may have received from the City that is either in my possession or otherwise directly or indirectly under my control.
- v.

Employee signature: _____

Employee name: _____

Date: _____

Department: _____