Information Systems Policy

Overview

The Information Systems policy provides the City of Marietta employees with a consistent standard regarding the access, use and care of the City's computer equipment, internetworking infrastructure, computer software, virus protection, internet access and electronic mail system.

The policy is separated into the following five sections for greater clarity and ease of reference.

1. Computer Equipment
2. Network and Application Access
3. Software and Virus Protection
4. Internet
5. E-Mail

Each policy section may contain one or more of the following areas:

- Policy Statement – terms and conditions regarding ownership, use and care
- Guidelines – general directions regarding use and care
- Standards – specific directions regarding use and care

Administration

This policy is to be administered by the City's department heads and or the appropriate appointing authority.

Computer Equipment

Policy Statement

All computers (desktop computers, laptops, servers), handheld computing devices (personal digital assistants, PalmPilot, Handspring Visor etc.), networking devices (routers, switches, hubs, wiring etc.), printing devices (desktop printers, workgroup printers, mail metering printers), scanning devices (faxes, scanners, multi-function printers) purchased with City funds and used to conduct City business are the property of the City and may only be used to conduct City business. All computing devices issued are the responsibility of the employee to whom they have been issued. All computing devices may be collected and examined at anytime and without notice. Misuse or abuse of the City's computer equipment may be grounds for employee disciplinary action and may result in termination.

Guidelines

- All computer equipment must be maintained and used in accordance with the manufacture's storage and use recommendations.
- All computer equipment must be protected from theft and vandalism through responsible storage and use.
- In the event of any intentional damage to City computer equipment or systems the employee will be held responsible for the cost of repair or replacement.

Network and Application Access

Policy Statement

The interconnection and intercommunication of all City computing equipment enables the effective completion of City business processes. All employees that have been granted access to the network are issued a username and password. It is the employee's responsibility to guard their username and password to protect themselves, other City employees and citizens from the interruption of City business and inappropriate access to City data. The use of the user's username and password is the sole responsibility of the user to whom the username is issued. The disclosure of an employee's username and password to anyone other than the employee's supervisor is strictly prohibited. It is the responsibility of the employee to know and understand the areas and resources available to them while using the interconnected equipment. Employees may not perform probing activities such as port scanning or random access attempts on any network resources. Inappropriate disclosure of one's username and password or the inappropriate access of data or resources may be grounds for employee disciplinary action and may result in employment termination.

Guidelines

- Use different passwords for all user accounts.
- Change passwords immediately if they may have been compromised.
- Be careful about where passwords are saved on computers. Some dialog boxes, such as those for remote access and other telephone connections, present an option to save or remember a password. Selecting this option poses a potential security threat

Standards

- All network access passwords will meet the following requirements
    1. Not contain all or part of the user's account name
    2. Be at least seven characters in length
    3. Contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphabetic characters (for example, !, $, #, %)
- All network access passwords will be changed every 90 days.
- Passwords may not be reused.
- No username and password may be written down on anything that is stored at or around the employee's equipment or work area.
- All application passwords must be changed on a periodic basis according to the department head's application password change requirements

Software and Virus Protection

Policy Statement

Only City owned software relating directly to the performance of the employee's job responsibilities may be used on an employee's computing equipment. City owned software may not be installed or used on an employee's home computing equipment except where specifically directed by the appropriate appointing authority. It is the responsibility of the employee to insure that virus protection software is enabled and functioning appropriately on his/her computing devices. Misuse or abuse of the City's software and virus protection systems may be grounds for employee disciplinary action and may result in employment termination.

Guidelines

- All media such as diskettes, CD's, Zip disks must be scanned for viruses upon access.

Standards

- Tampering with (decompilation or deinstallation) of City purchased software is strictly prohibited.
- Sufficient quantities of software licenses must be purchased in accordance with the intended use of the software.
- All computing devices must have installed and updated virus protection software or interact directly with virus protected systems that extend the virus protection to the connected device.
- Employees may not knowingly introduce viruses into the City's computing devices.

Internet

Policy Statement

Internet access shall be used for "official City business" only. Personal use or time spent for personal gain is strictly prohibited. Internet access for employees and computers is authorized through the department heads. Internet access is permitted through a user's account name and password and all use and/or misuse of internet access through the account are the sole responsibility of the account owner. If participating in internet accessible public forums, City employees may not state that something is or is not the City's official position without the express written approval of the appropriate supervisor. The search for and retrieval of sexually explicit material is strictly prohibited. The download and compilation of materials such as music or movies that is not directly related to the end user's job function is strictly prohibited. The City reserves the right to monitor and disclose all internet usage activity by its employees. Misuse or abuse of the City's Internet access may be grounds for employee disciplinary action and may result in employment termination.

Guidelines

- City employees may not permit other employees to use their computer for internet access without first completely logging off of the City's network.
- Hacking is the unauthorized attempt to gain access to computer resources. Hacking of computer systems is strictly prohibited.

Standards

- Almost all data and software accessible through the internet is subject to Federal copyright laws. The reuse of copyrighted material must follow the requirements of all applicable laws.
- Data accessed via the internet and used for official City business must be validated for accuracy through alternate methods such as a phone, e-mail or fax exchange with the data provider, or through and independent third party, where appropriate.
- Shareware and freeware application (Screen savers, Instant messaging clients etc.) download and installation is strictly prohibited unless for completion of specific City business functions and only when authorization is provided by the employee's department head.

E-Mail

Policy Statement

All electronic communications and stored information transmitted, received, or archived in the City's information system are the property of the City. The City reserves the right to access and disclose all electronic communications produced or received by its employees. All communications produced or distributed through the City's e-mail system are considered official City documents and are subject to the requirements of public record laws. Misuse or abuse of the City's e-mail system may be grounds for employee disciplinary action and may result in employment termination.

Guidelines

- Employees issued City e-mail accounts should check their "mailbox" at least twice daily.
- The use of the e-mail system is reserved solely for the conduct of City business. Solicitation for commercial ventures, religious or political causes, or other non-City-related solicitations are strictly prohibited.
- The receipt of personal e-mail messages not directly related to the execution of the employee's job responsibilities is strictly prohibited, and employees shall so advise senders of such messages.
- Notwithstanding the City's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them. Management personnel may permit their support staff access to their e-mail for administrative assistance.

Standards

- All Email should follow the same formality as a business letter and should contain the following:
  1. Short informative subject line
  2. Formal but friendly greeting
  3. Signature line containing contact information such as name, title and phone number
  4. A proprietary information and disclaimer statement
- Spelling, grammar and punctuation should be checked on all communications including files attached to e-mail messages.
- Professional language is required; abusive, harassing, threatening, sexual or ethnically oriented language, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, handicap or disability will not be tolerated.
- Sending messages to all employees of individual departments is prohibited unless the message is reviewed and approved by the department head.

- Sending messages to all City employees is prohibited unless reviewed and approved by the department head and then by the appropriate appointing authority.
- Informational and alert messages regarding personnel pay, benefits, health, application access or usage (e-mail, internet, network, etc.) that directly impact the employees may be sent by a department head or appropriate appointing authority to all affected employees without prior approval.

Statement of Acceptance

As an employee of the City of Marietta, I declare that I have read, understood and agree to abide by the City's Information Systems policy.

Signature of Employee: _____

Printed Employee Name: _____

Date Signed: _____