Information Technology
Security Policy and Procedures

Purpose

The purpose of this policy is to establish the minimum governance for information security, the acquisition and use of technology and services (computers, mobile devices, enterprise software, network resources) of the City of Marlborough (herein after “City”).

The Mayor of Marlborough has delegated the execution and maintenance of technology to the City’s Information Technology (IT) Director.

Table of Contents

Scope

This policy applies to all City employees, contractors, third-party associates, volunteers (herein after "Users") and all existing as well as future implementations of technology hardware, software and services.

The files/data created and stored on City or cloud assets for the purpose of conducting business are the property of the City and as such are subject to the policies set forth.

Assets and data that fall under the scope of the Criminal Justice Information Systems are also subject to the Criminal Justice Information Services (CJIS) Security Policy.
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Exceptions to Policy

Exceptions to this policy shall be made at the discretion of the City's IT Director. The IT Director shall ensure that the business need is valid, the risk level is acceptable and will conduct periodic reviews of all granted exceptions as needed.

Non-Compliance

Violations of this policy shall be treated like other allegations of wrongdoing at the City.

Allegations of misconduct related to this policy shall be adjudicated according to established procedures. Sanctions for inappropriate use on the City's systems and services may include, but are not limited to, one or more of the following:

- Temporary or permanent revocation of system access.
- Disciplinary action according to applicable City policies.
- Termination of employment; and/or
- Legal action according to applicable laws and contractual agreements.

Any questions relating to this policy should be directed to the IT Department, at 508-460-3762.

Definitions

802.11i – provides sophisticated authentication using a variety of protocols and strong security with the AES-CCMP encryption protocol

Antivirus software - A piece of software that is used to detect, delete and or neutralize computer-based viruses.

Advanced Authentication - is a multi-factor authentication solution that enables you to protect your sensitive data by using a more advanced way of authentication on top of the typical username and password authentication.

Blog - A component of a social networking or media site, usually maintained by an individual, with regular entries of commentary, opinions, or descriptions of events. Blogs are usually focused on a particular subject or area of interest. Blogs typically allow users to leave comments, and entries are usually displayed in reverse chronological order.

Cloud Services – IT services delivered over the internet and accessible globally from the internet.

Content - In the context of the internet and websites, content is the text, images, videos, and other usable information belonging to a website or a web page.

Comment - A response to a City news article or social media content, submitted by a commenter.

Commenter - A City official or member of the public who submits a comment for posting in response to the content of a particular City news article or social media content.

Electronic record means a public record whose creation, storage, and access require the use of an automated system or device. Ownership of the hardware, software, or media used to create, store, or access the electronic record has no bearing on a determination of whether such record is a public record.

Encryption - the process of transforming information to make it unreadable to anyone except those authorized to decode and read it.

ISP (Internet Service Provider) – is an organization that provides services for accessing, using, or participating in the Internet, for example your cable provider.

MAC (Media Access Control) Address – is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. MAC addresses are primarily assigned by device manufacturers and are therefore often referred to as the burned-in address. Your PC has a MAC Address.

Malware – Malicious computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

Virus- a software program capable of reproducing itself and usually capable of

causing great harm to files or other programs on the same computer
Trojans – Malware that appears to perform or performs a desired task for a user while performing a harmful task without the user's knowledge or consent.
Worms – a standalone malware computer program that replicates itself to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers.
Ransomware - Malware that holds the data of a computer user for ransom.

MFA (Multi-factor Authentication) - Your passwords can be easily compromised. MFA immediately increases your account security by requiring multiple forms of verification to prove your identity when signing into an application.

Peer-to-peer network – A computer network in which every computer acts as both a client and server, allowing every computer to exchange data and services with every other computer in the network.

Phishing - The act of sending email that falsely claims to be from a legitimate organization. This is usually combined with a threat or request for information: for example, that an account will close, a balance is due, or information is missing from an account. The email will ask the recipient to supply confidential information, such as bank account details, PINs or passwords; these details are then used by the owners of the website to conduct fraud.

Public Record - means recorded information that documents a transaction or activity by or with any public officer, agency or employee of an agency. Regardless of physical form or characteristic, the recorded information is a public record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of public business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is a public record.

Social Media - Content created by individuals using accessible and scalable technologies through the Internet. Examples of social media sites are Facebook, blogs, MySpace, YouTube, Twitter, and LinkedIn.

Social Network/Media Site - A website focused on building online forums or communities of people who share interests, activities, or opinions. Most are web-based and provide a variety of ways for users to interact, such as email, chat, instant messaging, and texting services. When this term is referred to, it shall be interpreted to include the site structure and all content contained on the site.

Social Media Site Administrator - Social media site administrators (SMSAs) are ultimately responsible for creating and maintaining their department social media sites. They create or approve social media communications, including managing delivery and publication of such communications in accordance with City policies, procedures, guidelines and standards, including maintaining necessary records. SMSAs are responsible for regularly reviewing all social media postings and responses, for keeping a record of all materials that are removed or not approved and reasons for such, the dates material was submitted and approved, and for tracking documentation on the site for

FOIA. Social media and networking sites must contain contact information for SMSAs.

SSID (Service Set Identifier) – is the primary name associated with an 802.11 wireless local area network (WLAN), including home networks and public hotspots. Client devices use this name to identify and join wireless networks. In simple terms, it's the name of your Wi-Fi network.

Secure Tunnel

FTP (File Transfer Protocol) - a program that allows files to be moved from one computer to another through the internet.

VPN (Virtual Private Network) - a secure way to connect to a private Network from a remote location, using the Internet. The VPN uses authentication to deny access to unauthorized users, and encryption to prevent unauthorized users from reading transmitted information.

SSL (Secure Socket Layer) - A security protocol to create confidential connections across the Internet

WPA (Wi-Fi Protected Access) - is a security protocol designed to create secure wireless (Wi-Fi) networks. It is similar to the WEP protocol but offers improvements in the way it handles security keys and the way users are authorized.

1. Acquisition Policy

Introduction:

All information technology hardware, software and services must be approved and/or acquired/purchased through the IT Department. This includes, but is not limited to, any “Off the Shelf” software, custom designed software applications or software enhancements with existing vendors, computers, scanners, printers, flash drives, mobile devices, cell phones and other peripherals. How the City acquires the technology is not relevant (via grant, donation, bundled with another purchase etc.). All computer hardware or software purchased without the prior approval of the IT Department will not be connected to the City’s network and will be returned to the vendor at the department’s expense.

1.1. Software:

All software will be purchased and installed through the IT Department or its designee.

1.2. Hardware:

All IT-related equipment and network dependent devices (ex. fax machines, copiers, scanners) must be purchased and installed through IT or its designee.

1.3. City Account:

All Users that require access to City computer systems must be correctly identified to control access to system resources. Every User is required to read and agree to follow the requirements set forth in this policy and all other City policies that apply.

All account creation, deletion, and changes are the responsibility of the IT Department. Only Human Resources can request an account. Users with accounts and thus access to City systems must complete annual security training.

It is the responsibility of the employee to protect the confidentiality of their account and password information (please also see Section 3. Password Policy).

2. Acceptable Use Policy

Introduction:

Since inappropriate use of City systems exposes the City to risk, this policy explains responsibilities for use of City IT resources (including but not limited to computer systems, email, the network, and the City’s Internet connection) and specifies the actions that are prohibited.

2.1. Acceptable Use:

Users shall use City systems to further the goals and objectives of the City. The types of activities that are encouraged include:

a. Performing job related functions as part of an individual’s assigned responsibilities.

b. Communicating with fellow employees, business partners of the City, and clients within the context of an individual’s assigned responsibilities.

c. Acquiring or sharing information necessary or related to the performance of an individual’s assigned responsibilities.

d. Participating in educational or professional development activities.

2.2. Unacceptable Use:

The use of technology resources is not to be used for purposes that could be reasonably expected to cause excessive strain that interferes with others’ productivity. Technology use at the City will comply with all Federal and State laws, all City policies, and ordinances. This includes, but is not limited to, the following:

a. Not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, discrimination, intimidation, forgery, impersonation, identity theft, gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading computer viruses).

b. Individuals should limit their personal use of the network. The City allows limited personal use for communication with family and friends, independent learning, and public service.

c. The City prohibits use for mass unsolicited mailings, access for non- employees to City resources or network facilities, uploading and downloading of programs, access to pornographic sites, personal relationship sites, gaming, political campaigns, endorsements, opinions or any other political activity, where citizens at large vote, solicitation of funds for commercial, personal, religious or charitable causes not sponsored by the City, competitive commercial activity or for profit activities unless pre-approved by the City, and the dissemination of chain letters.

d. Individuals may not establish City computers as participants in any peer-to-peer network, unless approved by the IT Department or their designee.

e. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications (e-mail, text, instant message, chat history etc.) belonging to the City or another individual without authorized permission.

3. Password Policy

Introduction:

All Users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. The City will continue to employ advanced authentication to ease the reliance on username/password and to stay current with industry standards for information security.

3.1. Password Construction:

a. Poor, weak passwords have the following characteristics:

i. The password contains less than fourteen (14) characters.

ii. The password is a common usage word such as:

- Computer terms and names, commands, sites, companies, hardware, software.
- The words "City of Marlborough", "city" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

b. Strong passwords have the following characteristics:

i. Contain both upper- and lower-case characters (e.g., a-z, A-Z)

ii. Have digits and punctuation characters as well as letters e.g., 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

iii. Are not based on personal information, names of family, etc.

iv. Passwords should never be written down.

3.2. Password Protection Standards:

a. Do not share City passwords with anyone, including administrative assistants or secretaries.

b. If an account or password is suspected to have been compromised, report the incident to the IT Department and change all passwords.

3.3. Minimum Requirements:

a. Minimum of fourteen (14) characters long

b. Must be changed every 365 days

3.4. Advanced Authentication:

a. When available systems shall use advanced authentication mechanisms (ie. 2 factor, single-sign on).

4. E-mail Policy

Introduction:

E-mail is a critical mechanism for business communications at the City. However, use of the City's e-mail system and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of the City.

4.1. Account Activation/Termination

a. E-mail access at the City is controlled through individual accounts and passwords. It is the responsibility of the employee to protect the confidentiality of their account credentials (please also see **3. Password Policy**).

b. All employees of the City can be provided with an e-mail account. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Possible non- employees that may be eligible for access include contractors, vendors, or agencies.

c. E-mail access will be terminated when the employee or third party terminates their association with the City, unless other arrangements are made. The City is under no obligation to store or forward the contents of an individual's e-mail account after the term of their employment has ceased.

4.2. City Representation

a. It is important to remember that an e-mail message is, in essence, a letter on organizational stationery; as such, commitments may be interpreted as commitments of the organization, and opinions may be taken as the opinion of the organization.

4.3. E-mail Etiquette

a. As use of e-mail grows, it becomes increasingly important for each e-mail user to use care and caution when sending messages to one another. The following advice is provided to all e-mail users when considering what is appropriate for sending in an e-mail message.

i. Ask yourself: would I want a jury to read this e-mail?
ii. Don't send offensive jokes or frivolous messages.
iii. Don't write anything you wouldn't want repeated.
iv. The content of the message should be something you would be comfortable saying in an open business meeting.
v. Reply All: Be aware when using the Reply All function and ensure your response is useful to everyone receiving the communication. Consider e-mailing the intended recipient directly using Reply.

4.4. Email Retention

a. The City retains all e-mail indefinitely.

4.5. Email Privacy

a. All e-mail users should be aware that confidentiality of electronic mail cannot be assured and that any communications which need to remain confidential should not be sent over the internet.

4.6. Monitoring and Confidentiality

a. The e-mail systems and services used at the City are owned by the City and are therefore its property. This gives the City the right to monitor e-mail traffic. While the City does not actively read e-mail, e-mail messages may be inadvertently read by IT staff during the normal course of managing the e-mail system.

b. In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with the City's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

c. If the City discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process.

d. Use extreme caution when communicating confidential or sensitive information via e-mail.

4.7. Non-City E-mail Accounts

a. The use of non-City or School e-mail accounts (accounts that do not end in @marlborough-ma.gov and @mps-edu.org) for City business is prohibited.

4.8. Reporting E-mail Incident

a. Any allegations of misuse should be promptly reported to the IT Department, 508-460-3762. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

4.9 Disclaimer

The City assumes no liability for direct and/or indirect damages arising from the user's use of the City's e-mail system and services. Users are solely responsible for the content they disseminate. The City is not responsible for any third-party claim, demand, or damage arising out of the use of the City's email system.

5. Data Protection Policy

Introduction:

Data protection provides a greater level of security than can be achieved with system-based protection methods (such as passwords) alone. Examples of data housed by the City include Intellectual Property, Personally Identifiable Information, financial, and any other data or information the City uses to conduct business with citizens and third parties. The City utilizes mechanisms and procedures to meet all federal and Massachusetts state laws/regulations regarding record retention and privacy.

Confidential Information/Personally Identifiable Information:

- Full Social Security Number (last 4 digits only are acceptable)
- Driver's License Number
- Financial account number or credit/debit card number
- Criminal history information
- State ID card number
- Passport number
- Personally identifiable medical information
- Tax Information
- Election information

Data that falls under the scope of the Criminal Justice Information Systems is also subject to the Criminal Justice Information Services (CJIS) Security Policy.
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

5.1. General Procedures:

a. All Confidential Information shall be protected to ensure the highest levels of security. Non-confidential information shall also be protected to ensure the highest levels of integrity and availability.

b. Only approved personnel can enter information into a City information system. Inputs shall be restricted according to granted permissions. The City utilizes least privilege in accordance with industry standards.

c. Users shall check entered information for accuracy, completeness, validity. These checks shall be performed at the point of data entry and periodic review as necessary.

d. Where possible, information systems shall protect the integrity and confidentiality of transmitted information using a variety of methods, such as: session authentication, session encryption or data encryption.

e. Always use good judgment in the creation, dissemination, storage, and retention of information of a personal, medical, or financial nature, where its release could jeopardize an individual's privacy or the best interests of the City as an organization, even if it does not fall within the technical definition of "confidential information." Consider whether there is a legitimate business purpose for creating the email or other record and whether it is safe to disseminate it. Safeguard the record appropriately given its sensitivity and be sure to follow the records retention schedule.

5.2. IT Procedures:

a. Where possible, systems should store Confidential Information in a secure manner using system or file level encryption.

b. Media destruction of storage devices (hard drives etc) shall be performed to ensure destruction of data once the media is no longer in use.

5.3. Data Handler/User Procedures:

a. Positively dispose of data that is no longer required according to authorized Records Retention Schedules.

b. Use software or hardware delete functions to remove non-confidential data from systems once that data is no longer required to be held according to authorized Record Retention Schedules.

c. Transmit Confidential Information in a secure manner using methods approves by the IT Department.

d. Encrypted tunnels should be used for all confidential electronic data transmissions i.e., Secure FTP, VPN, SSL (https).

e. Confidential Information shall never be sent unencrypted via Email.

f. Data should only be input according to established syntax parameters.

g. Inputted data should be checked for accuracy, authenticity, completeness, and validity.

5.4. Portable Media:

Portable media of the City within or upon which data can be stored. Specifically, it includes:

i. Removable magnetic media including external hard disk drives, external devices containing hard disk drives, floppy disks, and magnetic tape.
ii. Removable flash-based media including thumb drives, and flash cards.
iii. Optical media including DVDs and CDs.
iv. Paper and other printable materials.

a. All Confidential Information shall be protected to ensure the highest levels of security. Non-confidential information shall also be protected to ensure the highest levels of integrity and availability.

b. When information from the City's system is output to some form of portable media, that information and media must be handled and stored in a secure manner. It must be kept within a controlled area and access to that controlled area shall be physically restricted to authorized personnel.

c. Once portable electronic media is no longer needed to store or transport Confidential Information, it must be completely wiped before reuse in accordance with the IT Department's standards and methods.

d. Before allowing media to be transported, verify that a copy of the data stored on the media exists elsewhere in the City's network.

e. Portable electronic media from external sources shall not be introduced or re-introduced into any City owned or City network connected device without first being processed and approved by the IT Department.

6. Wireless Networks Policy

Introduction:

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the City's network. Only those wireless devices that meet the standards specified in this policy or are granted an exception by the IT Department are approved for wireless connectivity to the City's network.

6.1 Minimum Requirements:

a. Devices and wireless networks must only utilize the standards set forth in the 802.11i standard.

b. At minimum, WPA2 security specification for authentication and encryption.

c. Use City approved encryption protocols.

d. Maintain a hardware address (MAC address) that can be registered and tracked.

e. Users shall use discretion when using public wireless networks (Non-City maintained) to conduct City business.

7. Cellular Device Phone Policy

Introduction:

This policy establishes guidelines for the issuance and usage of City-owned cellular devices as well as procedures for monitoring and controlling costs related to cellular device use in connection with City business. This policy outlines guidelines for appropriate use, and other administrative issues relating to cellular device acquisition and reimbursement in order to enhance employee safety, limit City liability, and help manage cellular telecommunications costs.

7.1 Responsibility and Authority:

a. The IT Department in agreeance City management shall determine employee need for wireless phone services within their respective departments.

b. Employees and their respective departmental management are jointly responsible for understanding the terms of this policy.

7.2 Issuing a Cellular Telephone or Device:

a. The IT Director will be responsible for choosing and managing the best plan and equipment for the City.

7.3 General:

a. City-owned cellular devices are property of City and must be treated, used, and safeguarded as such. If a city provided cellular device is damaged, lost, or compromised the employee shall immediately notify the IT Department.

b. Cellular devices shall not be used for the purpose of illegal transactions, harassment, or obscene behavior, in addition to all other City policies.

c. City-owned cellular devices shall be subject to all applicable Massachusetts and federal Freedom of Information Act laws and regulations.

8. Remote Access Policy

Introduction:

This policy will define rules and requirements for connecting to the City's network from any remote location. These rules and requirements are designed to minimize the potential exposure to the City from damages which may result from unauthorized use of City resources.

8.1. General:

a. Remote access to the City's network shall utilize secure methods such as VPN, as determined and controlled by the IT Department.

b. Credentials and remote access shall not be shared with other individuals other than initially assigned by the IT Department.

c. Remote access shall only be granted with the approval of the IT Department.

d. If equipment (whether owned by the City or not) used for remote access to City systems and/or data is damaged, lost, or stolen, the authorized user shall immediately notify IT Department.

e. The remote access User accepts that their access and/or connection to the City's networks may be monitored to record dates, times, duration of access, and any other information deemed necessary by the IT Department.

f. The IT Department reserves the right to turn off, without notice, any access to the City's network that they deem may put the City's systems, data, or Users at risk.

9. Employee Social Media Policy

Introduction:

Our social media policy provides a framework for using social media. Social media is a place where people exchange information, opinions and experiences to learn, develop and have fun. Whether you're handling a city/school account or using one of your own, you should remain productive and avoid damaging the city or school system in any way. This policy provides practical advice to avoid issues that might arise by careless use of social media in the workplace.

Also, by "social media", we refer to a variety of online communities like blogs, social networks, chat rooms and forums – not just platforms like Facebook or Twitter.

This policy is built around two different elements: one, using personal social media at work and two, representing our city and school system through social media.

9.1. Personal Use:

a. We allow our employees to access their personal accounts at work. But we expect you to act responsibly and ensure your productivity isn't affected.

b. Adhere to the City's confidentiality policies. We also caution you to avoid posting something that might make your collaboration with your colleagues more difficult (e.g. hate speech against groups where colleagues belong to).

c. Ensure others know that your personal account or statements don't represent the City or school system. Do not state or imply that your personal opinions and content are authorized or endorsed by the City or school system. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings.

d. Avoid sharing intellectual property like trademarks on a personal account without approval.

Confidentiality policies and laws always apply.

9.2. City or School Representation:

a. Some employees represent our city and school system by handling social media accounts that speak on our city or school system's behalf. When you're sitting behind a city or school social media account, we expect you to act carefully and responsibly to protect our city and school system's image and reputation.

b. Be respectful, polite and patient, when engaging in conversations on our city and school system's behalf. You should be extra careful when making declarations or promises towards customers, parents, the public, and all other stakeholders.

c. Avoid speaking on matters outside your field of expertise when possible. Everyone should be careful not to answer questions or make statements that fall under somebody else's responsibility.

d. Inform the Mayor's office when you're about to share any major-impact content.

e. Avoid deleting or ignoring comments for no reason. They should listen and reply to criticism.

f. Never post discriminatory, offensive or libelous content and commentary.

g. Correct or remove any misleading or false content as quickly as possible.