IT Policy Manual

Jordan Turek, PhD
Information Technology Director

Adopted and Approved by:

David T Harden
City Manager

06/26/2019
Date

Implementation Information and Revision History

Implementation Information:

Review Frequency:	Annual
Responsible Person:	Director, IT
Approved By:	City Manager
Approval Date:	June 26, 2019

Revision History:

Version:	Date:	Description:
1.0	6-1-2018	• Initial IT Policy Manual • Approved and Adopted by CM G. Polanco
1.1	06-26-2019	• Minor Grammatical Updates • Re-Approved by CM D. Harden

Table of Contents

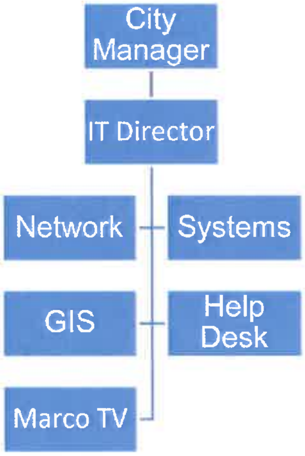
Policy 1.0 - Governance Policy

1.1 Policy

The purpose of Information Technology (IT) Department governance is to align the roles and responsibilities of the I.T. Department with the roles and responsibilities of all the City's departments.

1.2 Management and Organization

The Information Technology Department reports to the City Manager.



1.3 Vision

Enabling access to City Government, making it available to anyone, at any time, from anywhere.

1.4 Mission

The I.T. Department is committed to delivering technological solutions to provide citizens, businesses, and city employees with convenient access to information and services in a cost-effective manner.

1.5 Responsibilities

I.T. Department -

The primary responsibility of the I.T. Department is to align I.T. with business goals, implement new technology, control I.T. costs, increase efficiencies, ensure data security and integrity, and provide systems and end-user support for all information technology functions in the City of Marco Island Government. The majority of the tasks performed fall into three programs; Support, Research & Development, and Training.

Technical Support: Most of the work performed by the I.T. Department falls under this program. It encompasses all helpdesk activities, hardware replacement and upgrades, software installation and upgrades, system administration, and support of communication systems such as the IP Telephony phone systems, cellular phones, and analog devices.

1.5 Responsibilities – (CONTINUED)

Research & Development: Through this program new technology is evaluated, purchased, and implemented. As technology changes, and the role technology plays in our government's daily activities change, we need to continuously assess the application of that technology, insuring that we implement solutions that improve job efficiency and meet all regulatory requirements. Through this program the I.T. Department works with other City departments to find the technology solutions that best meet their needs.

Training: As technology changes so do the skills required to support and use it. This program provides for the ongoing skills training of I.T. Department staff and assists other departments in providing end-user training tailored to the needs of their staff. The I.T. Department will sponsor in-house training on applications and systems specific to the needs of our City, as well as outsource training where necessary.

City Manager - Provide oversight to the I.T. Department

1.6 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 2.0 - Information Technology Advisory Committee

2.1 Policy

The City of Marco Island will establish and maintain an Information Technology Advisory Committee (ITAC).

2.2 Mission of the Committee

The mission of the ITAC is to advise and assist on technology and telecommunications matters that have a major impact on City staff as well as the community, and facilitate communications among citizens, city council, city staff, and the Information Technology Department staff.

2.3 Functions of the Committee

- Make recommendations to the Information Technology Department with the purpose of increasing the effectiveness of technology and telecommunications policies and programs.
- Provide input on current developments and future opportunities in the area of technology, e-government, and regulatory activities.
- Advocate participation in technology and telecommunications policy formulation and implementation.
- Increase awareness among staff of opportunities to be found in technology and telecommunications uses.

2.4 Membership

The Committee shall consist of all Department Heads, the IT Director, and additionally any Middle Managers and IT staff recommended by the aforementioned.

2.5 Meetings

Meetings shall be held at a location and time acceptable to a majority of the Committee. The Committee shall meet as often as necessary to complete its business. The I.T. Department Manager shall act as Chairperson of the Committee. The Chairperson will appoint a committee member to take minutes of the meetings.

2.6 Meeting Agenda's and Minutes

An agenda for the meetings will be generated by the I.T. Department. Minutes of the meetings will be produced and forwarded to all committee members within 30 days after a meeting.

2.7 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 3.0 - Computer Hardware

3.1 Policy

All computer hardware purchased for use within the City shall be authorized by the I.T. Department.

3.2 Purpose/Description

I.T. will authorize all purchases and installation of all computer hardware to ensure conformance to City technical standards, to meet computer security requirements, and to interface properly with other computerized equipment at the City. Employee-owned hardware may not be connected to the City network without prior authorization by the I.T. Department.

3.3 Enforcement

The Finance Director will reject all requests for computer hardware that are not approved by the I.T. Department. Any computer hardware found to be in use without I.T. approval will be disconnected immediately. The incident will be reported to the violator's Department Head and may result in disciplinary action.

3.4 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Work with I.T. to determine hardware needs and to develop an appropriate annual budget. Obtain I.T. approval to purchase any hardware prior to doing so.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

Finance Director – Ensure that the I.T. Department has authorized all requests for computer hardware.

I.T. Department - I.T. must authorize all purchases and installation of all computer hardware. I.T. will maintain and periodically inventory all hardware within the City to confirm policy enforcement and to provide for verification of fixed asset tracking for insurance purposes.

3.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 4.0 - Computer Software

4.1 Policy

All computer software purchased or downloaded for use within the City shall be authorized and installed by the I.T. Department. I.T. will also provide for the maintenance of any packaged software and upgrade that software as needed. This policy applies to all operating system software as well as application software.

4.2 Purpose/Description

I.T. will authorize and install city-owned computer software to ensure conformance to City technical standards, to meet computer security requirements, and to interface properly with other computerized hardware and/or software within the City as required. Employee-owned software may not be connected to the City network.

4.3 Software Acquisition

It is the policy of the City of Marco Island to always purchase packaged software unless there is an overwhelming business need to create a custom package. The I.T. Department does not have the resources to develop or maintain custom software packages.

All proprietary software purchases must provide for escrowing of software source code.

All software packages must be purchased with software maintenance agreements that will be maintained by the I.T. Department.

Acquiring software is a joint responsibility between the I.T. Department and the using department. The using department is responsible for ensuring the software will meet their functional needs. I.T. will ensure the software can technically operate in the City's environment and provide cost and budget information into the decision making process.

4.4 Enforcement

The Finance Director will reject all requests for computer software that is not authorized by I.T.. Any computer software found to be in use without I.T. approval will be removed immediately. The incident will be reported to the violator's Department Head and may result in disciplinary action.

4.5 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Work with I.T. as an equal partner in the acquisition process. The using department will provide a primary and secondary liaison to the software vendor for direct application support. The I.T. Department will assist the using department with unresolved support issues.

4.5 Responsibilities (CONTINUED)

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

Finance Director – Ensure that the I.T. Department has authorized all requests for computer software.

I.T. Department – Work with using department as an equal partner in the acquisition process. Maintain the software in an operational state, including software upgrades, patches, and fixes. Ensure renewal of all support agreements. Assist the end-user with application support issues when the end-user is unable to resolve issues directly with the software vendor.

4.6 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 5.0 - E-mail

5.1 Policy

The City encourages the business use of e-mail as a productivity enhancement tool. E-mail access will be granted to all City employees unless specifically denied by the employee's Department Head and/or the City Manager.

5.2 Purpose/Description

The purpose of this policy is to clearly define the acceptable use of the City's e-mail system and what actions are prohibited.

5.3 Ownership of the E-mail System

The City's e-mail system belongs to the City of Marco Island and the contents of all e-mail communication are accessible at all times by the City, with or without advance notice. Nothing in or on the e-mail system should be considered confidential. The employee has no right to privacy of e-mail.

5.4 Acceptable Use

Use of the City's e-mail system is intended for City related business. All employees are to use e-mail as they would any other type of official City communications tool. When any e-mail is transmitted, both the reader and sender should consider if the communication falls within ethical guidelines. No communication should contain confidential information. Communication by e-mail is encouraged when it results in the most efficient and/or effective means of communication.

City employees are permitted incidental and occasional personal use of the e-mail system, and such use will be treated the same as other business related e-mail messages. The following are guidelines when using the City's e-mail system for personal use:

- Personal incoming or outgoing e-mail must be kept to a minimum so that it does not consume more than a trivial amount of system resources
- Personal incoming or outgoing e-mail must not interfere with an employee's productivity
- Personal use of the e-mail system is a privilege that may be monitored, restricted, or revoked at any time.

5.5 Prohibited Uses

The following uses are prohibited:

- Charitable or fundraising campaigns unless specifically approved in advance by the City Manager

- Solicitations or proselytization (defined as: campaigning, preaching, or evangelizing) for commercial ventures, chain letters, religious or personal causes, or outside organizations or other similar, non job-related solicitations

5.5 Prohibited Uses (CONTINUED)

- E-mails that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale. Examples of forbidden transmissions include sexually-explicit messages, gambling, cartoons, or jokes; unwelcome propositions or love letters; ethnic or racial slurs; or any other message that may be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, religious or political beliefs

- Use of e-mail to send copies of documents in violation of copyright laws

- Use of the e-mail system to compromise the integrity of the City or its business in any way

- Use of e-mail to offer for sale non-City related items. The Employee Newsletter, which provides a "For Sale" section and is distributed internally via City e-mail, is excluded.

5.6 Retention of E-mail

All incoming and outgoing email is archived on the archiving server and is searchable by the City Clerk and IT Staff for public records requests. User mailboxes will have a mailbox quota to limit the amount of email retained on the email server in order to improve performance.

5.7 Mailbox Limits

The I.T. Department will set mailbox and message size limits that are appropriate to the stability and adequate performance of the e-mail system.

5.8 Enforcement

The I.T. Department will provide for the enforcement of these policies through the use of monitoring technology and report violations to the Department Head of the offending employee for disciplinary action, if necessary.

5.9 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Must maintain e-mails in accordance with State of Florida Public Records Laws. Must coordinate long-term storage with the I.T. Department, when necessary.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Manage mailbox limits. Monitor and report violations.

5.10 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 6.0 - Internet

6.1 Purpose and Description

The City encourages the business use of Internet access as a productivity enhancement tool. Internet access will be granted to all City employees unless specifically denied by the employee's Department Head and/or City Manager.

6.2 Acceptable Use

Use of the City's Internet access is intended for City related business. All employees are to use Internet as they would any other type of official City tool. Users should consider ethical guidelines.

City employees are permitted incidental and occasional personal use of the City's Internet system, and such use will be treated the same as any other legitimate business access. The following are guidelines when using the City's Internet system for personal use:

- Personal usage must be kept to a minimum so that it does not consume more than a trivial amount of system resources
- Personal usage must not interfere with an employee's productivity
- Personal use of the City's Internet is a privilege that may be monitored, restricted, or revoked at any time.

6.3 Prohibited Use

Any use of the Internet for "moonlighting", soliciting for commercial ventures, gambling, religious or personal causes, or outside organizations, or for other similar non job-related solicitations is strictly prohibited. Use of the City's Internet to access any site or material that is sexually explicit, pornographic, obscene, that may be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, or religious or political beliefs, or has the potential to cause the City public harm or disrepute is strictly prohibited.

Users shall not install any browser plug-in or "enhancement applications" such as Flash, Real Media, Quick Time, Shock Wave, browser toolbars, etc., without permission by the I.T. Department. This includes, but is not limited to: pop-up blockers, anti-spyware programs, screen savers, background changers, or any other item that is not provided by the I.T. Department as part of the original system configuration or added by IT.

6.4 Security and Blocked Access

The I.T. Department will provide for Internet security that includes, but is not limited to, firewall protection, specific routing, profiles, and passwords. Web sites that have no legitimate business purpose may be blocked from access. All web and internet traffic may be blocked from access until a specific business use is demonstrated. An audit trail of access to sites may be maintained by the I.T. Department to investigate possible violation of City policy or breach of security.

6.5 Public Representation

No media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, or any other public representation about the City of Marco Island may be issued unless appropriate management has granted approval.

6.6 Enforcement

The I.T. Department will monitor Internet access through the use of technology tools. Violations will be reported to the Department Head and/or the City Manager of the offending employee for disciplinary action, if necessary.

6.7 Responsibilities

End-Users – Must be aware of these policies and ensure compliance.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Manage Internet security. Monitor and report violations.

6.8 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 7.0 - Access to Computer Systems

7.1 Policy

It is the policy of the City of Marco Island to only grant access to systems and programs that are required in the performance of an individual's job. Temporary access will be granted to individuals on a temporary basis when filling in for someone on vacation or other leaves of absence, and to outside parties for the purposes of fulfilling their obligations to the City. Department Heads must authorize access to systems and software under their control.

7.2 Purpose/Description

The purpose of this policy is to ensure that individuals only have access to the software and systems that are required to perform their duties. This minimizes the risk of internal security violations.

7.3 Enforcement

Access authorization documentation will be generated for each individual indicating what software and/or systems are to be accessed and what privileges (read, write, etc.) are permitted. I.T. will ensure that only authorized rights and privileges are granted to the employee. Violations will be reported to the Department Head of the offending employee for disciplinary action, if necessary.

7.4 Responsibilities

End-Users - Must be aware of these policies and ensure compliance.

Department Heads – Provide written authorization for access rights and privileges to the I.T. Department on an I.T. Authorization Form or via ticket submitted to the City's work order system. Annually review and reconfirm accuracy of access rights and privileges. Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Grant rights and privileges for system access based upon submission of Form 7-1 from an authorized individual. Manage and audit user access rights.

7.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 8.0 - Password Security

8.1 Policy

All City computer systems are user identification (UID) and password protected to identify who is using the system and what rights and privileges they may have within the system.

8.2 Purpose/Description

All City computer systems are protected by UID and passwords. City computer systems may monitor access by UID and records can show such information as who logged in, when they logged in, and what they accessed on the system.

It is the responsibility of the user to protect his/her password as they would any other identification number such as social security number, credit card number or other such personal information. Passwords shouldn't be shared; however, should users share their passwords with others, the users assume full responsibility. In the event passwords are written, they must be kept in a secure location.

8.3 General Requirements

Passwords must meet minimum complexity requirements. Passwords must be at least eight (8) characters long, must not contain any part of the user's name, must include three of the following four categories: uppercase characters, lowercase characters, numbers, non-alphanumeric characters such as ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/. Password requirements for applications may vary.

Passwords for network access login must not duplicate any other accounts outside of the city network (i.e. Apple ID, department specific applications, vendor website, etc.)

Passwords must not be duplicated on personal computers systems and personal accounts.

Passwords must not be inserted into email messages and other forms of electronic communication.

Do not reveal a password over the phone to ANYONE.
Do not reveal a password in an email message.
Do not reveal a password in front of others.
Do not reveal a password on questionnaires or security forms or other documents.
Do not share a password with family members.
Do not reveal a password to co-workers.

If someone demands a password, refer them to this policy document or have them call the IT Department. If an account or password is suspected to have been comprised, report the incident to the IT Department staff and change all passwords.

Password auditing may be performed on a periodic or random basis by the IT Department staff or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it or the account may be disabled.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure against "dictionary attacks". A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. All of the rules above that apply to passwords apply to passphrases.

8.4 Password Expirations

Network logon passwords will expire on a 90-day basis and must be changed. Users may not reuse the last 10 network logon passwords.

8.5 Enforcement

I.T. will monitor the use of UID and passwords to ensure only authorized users access the system and to determine that passwords have not been written down and left in unsecured locations. Violations of this policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

8.6 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Follow password policy requirements and maintain confidentiality of UID and passwords.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Issue passwords with proper authorization and monitor compliance with the policy.

8.7 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 9.0 – Data File Storage

9.1 Policy

End-users shall store data files on the City's network servers in designated locations.

9.2 Purpose/Description

The purpose of this policy is to ensure that individuals save data files in designated locations to ensure daily backup of files to tape or other media for purposes of restoration in the event of a disaster or other unforeseen circumstance. Files stored locally on end-user systems cannot be recovered in the event of a system crash. Therefore, the IT Department strongly recommends the use of designated network server locations to store any and all files required by an end-user to perform their job duties.

9.3 Enforcement

Should the I.T. Department find City data files on an end-user's computer, I.T. staff will assist end-users with relocating files to a network server. In the event of a system crash, the IT staff will only provide minimal data recovery support and is not obligated to restore lost system files that are not backed up or stored according to this policy. Continued violations of this policy may be reported to the Department Head for disciplinary action, if necessary.

9.4 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Must save all data files in designated locations on network file servers.

Department Heads –Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Assist end-users with relocating files to network servers. No obligation to restore or recover locally stored files from end-user desktops or laptops. Report violations to Department Heads.

9.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 10.0 - Public Records Request

10.1 Policy

It is the policy of the City of Marco Island to direct all computer system public records requests to the City Clerk pursuant to the City of Marco Island Records Management Plan.

10.2 Purpose/Description

Although much of the information generated by a City is subject to public records requests, there are a number of exceptions that are provided for in Chapter 119 of the Florida State Statutes. Disseminating information that is subject to these exceptions is a serious violation of State law. All public records requests for electronic records should be forwarded to the City Clerk, or designee, for proper handling. No end-user should provide electronic information to any individual without first obtaining authorization from the City Clerk or designee.

10.3 Enforcement

Employees are expected to follow this policy. Violations of this policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

10.4 Responsibilities

End-Users - Must be aware of these policies and ensure compliance. Redirect electronic public records request to the City's Clerks office.

City Clerk – Receive and process request in accordance with Florida State Statutes and the City of Marco Island Records Management Plan. Designate fulfillment duties for the request to the appropriate department staff member if desired.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Assist City Clerk or designee with compiling electronic public records requests when needed.

10.5 Policy History

Adopted: 6/1/2018	Approval: City Manager

Policy 11.0 - Instant Messaging/Chat/Text

11.1 Policy

Instant Messaging and all related tools (voice chat, file transfer and sharing, etc.) are prohibited on City computers and/or city tablets, phones, mobile devices, etc. with the exception of authorized messaging software for internal use only.

11.2 Purpose/Description

External instant messaging/chat is prohibited due to the inherent security risks associated with these programs. The I.T. Department may provide messaging software for internal use only. All internal Instant Messaging chat sessions will be logged for the sole purpose of accommodating public record requests. The messages will be retained for a period of time in accordance with the State of Florida General Records Schedules. Employees are to assume there is no right to privacy for electronic communications on the City's communication devices

11.3 Enforcement

Any instant messaging/chat software found to be in use without I.T. approval will be immediately removed. Instant messaging/chat websites may be blocked. The incident will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

11.4 Responsibilities

End Users – Must be aware of these policies and ensure compliance. Shall not install or utilize instant messaging/chat programs, websites, etc.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Monitor activity, remove and confiscate unauthorized instant messaging/chat software, block access to instant messaging/chat websites, and report violations.

11.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 12.0 - Importing External Data

12.1 Policy

Importing data files for currently supported applications on City owned computers is permitted under certain conditions. Data files for applications not currently supported must be reviewed by the I.T. Department prior to importing.

12.2 Purpose/Description

This policy relates to the importing or copying of any file that does not already reside on a City computer. Importing files of any currently supported application is permitted via the following methods: CD, USB drive, or e-mail. Images (photos) on digital camera media may be imported to City computers.

All other files must be authorized by the I.T. Department prior to importing.

Supported applications include, but are not limited to, Microsoft Word (.doc, .dot, .rtf, .txt), Microsoft Excel (.xls), Microsoft PowerPoint (.ppt), Microsoft Access (.mdb), Microsoft Publisher (.pub), Microsoft Outlook (.eml, .pst), Adobe Acrobat (.pdf), and Adobe Photoshop (.psd, .bmp, .gif, .jpg).

Other file types may pose a significant threat to the City's computer system and are not permitted to be imported without authorization from the I.T. Department. These file types include, but are not limited to, the following:

- Archives/Compressed - .cab, .gz, .gzip, .jar, .rar, .rpm, .tar, .tgz, .z, .zip
- Executables - .bat, .chm, .class, .cmd, .com, .dll, .drv, .exe, .lnk, .ocx, .pif, .reg, .scr, .sys, .vxd
- Scripts - .asp, .hta, .htx, .js, .php, .php3, .vb, .vbs, .ws, .wsc, .wsf, .wsh, .wst

All imported files must be manually scanned for viruses using the local anti-virus software by the end-user before accessing the files.

12.3 Enforcement

It is expected that employees will adhere to the policy. Violations of this policy will be reported to the Department Head for disciplinary action, if necessary.

12.4 Responsibilities

End-Users - Must be aware of these policies and ensure compliance. When necessary, work with I.T. to import non-supported data files and ensuring manual virus scans are completed prior to access.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

12.4 Responsibilities (CONTINUED)

I.T. Department – Work with employees who have a need to import data files that have potential hazards. Report violations.

12.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 13.0 – Digital Data Backup and Recovery

13.1 Policy

Data files maintained on the network servers will be routinely backed up to electronic media and / or locations offsite of the data center, for the sole purpose of restoration, not preservation.

13.2 Purpose/Description

Information Technology will conduct backups of critical data on a Daily basis. Backups will be conducted on a more frequent schedule when possible. Disk backup appliance and media will be stored for the designated period of time stated below and will be used for restoration in the event of a disaster.

13.3 Backup Audit Logs

The I.T. Department will maintain a log of all backup jobs within the backup software.

13.4 Backup Job Schedule

Disk Backups will be performed as frequently as possible throughout the day while limiting the impact on system performance.

No backup job shall be kept on disk for more than three months. Backups of servers with limited changes shall only be kept on disk for 30 days. In the event of a disaster requiring system restoration from backup media, information processed that day, or since the last good backup, may be lost and will be the responsibility of the user to re-process.

13.5 Enforcement

The I.T. Department will periodically audit the backup logs to ensure the backups are properly maintained and stored by I.T. staff. Continued violations of this policy will result in disciplinary action.

13.6 Responsibilities

End Users – Must be aware of these policies and ensure compliance. Responsible for notifying the I.T. Department immediately upon determining that data may be lost and need to be restored from backup media.

Department Head – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Provide for backup of network data, maintain appropriate electronic logs, and store backup media offsite. Report any user violations to the Department Head for action.

13.7 Policy History

Adopted: 6/1/2018	Approval: City Manager

Policy 14.0 – Remote/Mobile Network Access

14.1 Policy

The City will only grant remote access to end-users for systems and programs that are required in the performance of their job.

14.2 Purpose/Description

The policy provides a secure means for end-users to access programs and data from outside of the City's network. It also ensures integrity and security of network and systems by minimizing threats and vulnerabilities associated with access to systems via external networks.

14.3 Enforcement

Department Heads must authorize all remote access in writing on an I.T. Authorization Form or via ticket submitted to the City's work order system. The I.T. Department will provide for the enforcement of these policies through the use of mobility management software and other technology tools.

14.4 Responsibilities

End Users – Must be aware of these policies and ensure compliance. Shall not utilize any mobile technology device without authorization by the Department Head and the I.T. Department. Shall maintain physical security of remote/mobile devices and protect them from physical intrusion, theft, loss, fire, hazardous materials, flood, and other damages. Shall report all incidents to the IT Department immediately.

Department Heads – Provide written authorization for access rights and privileges to the I.T. Department on an I.T. Authorization Form or via ticket submitted to the City's work order system. Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Procure, configure, and install authorized remote/mobile devices with latest security measures as determined necessary for connectivity to the City network. Monitor remote access to the City network to thwart attempts of unauthorized access and to ensure access control methods are effective.

14.5 Policy History

Adopted: 6/1/2018	Approval: City Manager

Policy 15.0 – Voice Mail

15.1 Policy

The City provides voice mail access to all City employees with desk phone and/or cell phone access unless specifically denied by the employee's Department Head and/or City Manager. Voice Mail is an enhanced feature of desk phones and cell phones and should be utilized as any other communications tool.

15.2 Purpose/Description

The purpose of this policy is to clearly define the acceptable use of the City's voice mail systems, and establish voice mail storage and retrieval guidelines. Employees are to assume there is no right to privacy for electronic communications on City communication devices.

15.3 Acceptable Use

Use of the City's voice mail system is intended for City related business. All employees issued voice mail boxes are to use them as they would any other type of official City communications tool. No communication should contain confidential information. Communication by voice mail is encouraged when it results in the most efficient and/or effective means of communication.

At their supervisor's discretion, incidental and occasional personal use of the voice mail system is permitted by the City employees, but these communications will be treated the same as other business related communications. The following are guidelines when using the City's voice mail systems for personal use:

- Personal incoming or outgoing cell calls must be kept to a minimum so that it does not result in additional cost to the City above the normal monthly telephone operational expense.
- Storage and management of personal incoming or voice mail calls must not interfere with an employee's productivity and must not utilize any more than a nominal amount of storage space on the City's voice mail system.
- Personal use of the voice mail system is a privilege that may be monitored, restricted, or revoked at any time.

15.4 Prohibited Uses

The following uses are prohibited:

- Charitable or fundraising campaigns unless specifically approved in advance by the City Manager

- Solicitations or proselytization for commercial ventures, religious or personal causes, or outside organizations or other similar, non job-related solicitations

15.4 Prohibited Uses (CONTINUED)

- Communications that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale. Examples of forbidden voice mail communications include sexually-explicit messages; inappropriate jokes; unwelcome propositions; ethnic or racial slurs; or any other communication that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, religious or political beliefs

- Use of the City's voice mail in any way that compromises the integrity of the City or its business

- Use of voice mail to offer for sale non-City related items

15.5 Abusive Use

All City voice mail boxes are subject to internal and external audits. Abusing the use of City voice mail will result in the suspension of voice mail box privileges and may lead to other disciplinary actions.

15.6 Storage

The IT Department will determine the amount of voice mail system storage necessary to adequately meet the needs of the users while balancing the impact of the storage on the phone system.

Default voicemail storage is 20 minutes of voice recording time total, not a set number of messages. This can be increased on an individual basis by submitting a request through the IT work order system.

15.7 Access and Retention

End-users may access their voice mail messages through the WAVE application. Voice mail messages are typically considered as transitory messages under Chapter 119 of the State of Florida public records laws. Transitory records are created primarily to communicate information of short-term value, and they are not intended to formalize or perpetuate knowledge and do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt.

Should end-users determine that a voice mail record does indeed meet retention requirements under the public records law, they will need to access the voice mail message through the WAVE application, and export it as a .wav file to their user folder for retention until destruction date is reached.

15.8 Enforcement

The I.T. Department will provide for the enforcement of these policies through monitoring voice mail box usage and reporting violations to the Department Head for disciplinary action, if necessary.

15.9 Responsibilities

<u>End-Users</u> – Store voice mails that have retention requirements within their user folders outside of the voice mail system. Must be aware of these policies and ensure compliance.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department - Monitor usage and report violations.

15.10 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 16.0 – Security Incident Response

16.1 Policy

The I.T. Department will respond to computer security incidents, which may occur within the City of Marco Island government.

16.2 Purpose/Description

The purpose of this policy is to clearly define the roles, responsibilities, and communications procedures for responding to computer security incidents, and to detail the incident classifications.

16.3 Scope

Computer security incident response policy is applicable to all City information and infrastructure computing resources, at all levels of sensitivity, whether owned and operated by the City or operated on behalf of the City.

16.4 Leadership Role

Computer security incident response management shall be provided by the I.T. Director, and support members may include the Network Administrator, Human Resources, Police Chief, City Manager and/or others as deemed necessary.

Computer security incident response management is for the purpose of investigating an apparent information security incident and to minimize damage to the City's computer systems.

The role of the I.T. Director or designee is to respond rapidly to any suspected security incident by identifying and controlling the suspected incident, notifying end-users of proper procedures to preserve evidence, and report all findings to the City Manager.

16.5 Computer Security Incident Classification

16.5.1 Identifying Computer Security Incidents

A security incident is any event resulting in the City's computer systems, networks, or data being viewed, manipulated, damaged, destroyed, or made inaccessible by any unauthorized activity.

16.5.2 Notification of Computer Security Incidents

Successful incident handling requires employees to immediately contact the I.T. Department to report incidents. Contact should be made by phone or in person without delay.

16.5.3 Classification of Computer Security Incidents

It is the responsibility of the I.T. Department to classify security incidents into two classes based on the severity of incident: Class 1 and Class 2.

Class 1 Incidents: Localized and/or Minor.

Examples of Class 1 incidents are:

- Localized virus attacks, Spam, Malware, phishing and/or spear-phishing
- Internet abuse, excluding criminal behavior
- Incidents traceable to user error or system failure
- Minor attempts at intrusion, scanning, or pinging
- Missing I.T. devices or equipment
- Theft of I.T. devices

Class 2 Incidents: City-wide and/or High Impact.

Examples of Class 2 incidents are:

- Coordinated, distributed attacks
- Any attacks which cause denial of service
- Financial fraud involving computers
- Unauthorized activity involving a file server or host
- Theft of proprietary information
- Unauthorized activity involving any sensitive system (Financials, Public Safety, IT, etc.)
- Internet abuses which violate either Federal or State law
- Web defacement
- Customer data compromised

16.6 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Report any suspicious activity to the I.T. Department by phone or in person without delay. Document actions taken prior to awareness of suspicious activity.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department –

- Evaluate incident to make initial determination of classification/severity and notify City Manager of Class 2 events.
- Inform all other users who are affected by the security incident of the necessary actions to control the incident.
- Share with City personnel relevant information regarding security trends, local or widespread attacks, and general security best practices
- Determine if criminal investigation support is needed.
- Perform appropriate back tracing, technical analysis and other tasks required by the review.
- Report periodic status of the Class 2 incidents to the City Manager.
- Conduct a debriefing of lessons learned. Prepare subsequent report including root causes, actions taken to resolve incident, and recommendations for prevention of similar incidents. Submit report to the City Manager.

16.7 Policy History

Adopted: 6/1/2018   Approval: City Manager

Policy 17.0 - Architectural Standards

17.1 Policy

This policy establishes the City of Marco Island's technical architecture as the primary source for providing information technology technical requirements which govern the acquisition, use and management of information technology resources by City staff.

17.2 Purpose/Description

The City of Marco Island's Enterprise Architecture is a strategic asset used to manage and align the City's business processes and I.T. infrastructure/solutions with the City's overall strategy.

It is the intent to standardize and simplify the many technologies and products used in order to ensure continuity of operations, reduce staffing cost, and to build a reliable computer environment.

17.3 Hardware and Software Standards

17.3.1 Server Operating Systems

The I.T. Department will continually evaluate the newest release of the Microsoft, Linux and other server operating systems for compatibility, functionality and business need. Upgrades will be implemented as determined feasible by the I.T. Department within the constraints of the budget and available resources.

17.3.2 Desktop Client Operating Systems

The I.T. Department will continually evaluate the newest release of the Microsoft, Linux, and Apple (Mac) desktop operating systems for compatibility, functionality and business need. Upgrades will be implemented as determined feasible by the I.T. Department within the constraints of the budget and available resources.

17.3.3 Productivity Applications

The I.T. Department will continually evaluate the newest release of productivity applications for compatibility, functionality and business need. Upgrades will be implemented as determined feasible by the I.T. Department within the constraints of the budget and available resources.

17.3.4 Network Infrastructure

The I.T. Department will continually standardize the network infrastructure on industry accepted, high performance, best of breed infrastructure products and protocol standards. The uniformity of this type of equipment will provide stability to the City's network infrastructure as well as Internet accessibility and connectivity.

17.3.5 Security as a Platform Decision Factor

The I.T. Department will consider business security requirements up front when making decisions for all platforms from personal computing devices to enterprise servers.

17.3.6 Remote Administration Platforms

The I.T. Department shall acquire platforms designed for ease of remote administration, diagnosis, and systems management.

17.3.7 Cabling Standards

The City will utilize Information Transport Standards (ITS) for all new facility information and communications cabling installations to ensure compatibility and integrity.

17.3.8 Personal Computing

17.3.8.1 Centralized Personal Computing Decisions

The I.T. Department shall centralize personal computing decisions regarding what shall be procured, how frequently devices may be refreshed, how agency support is to be provided, what security methods are acceptable, and what methods of access may be used.

17.3.8.2 Personal Computing Security Software

The I.T. Department shall establish the minimum requirements for the base image to be used on personal computers, to include the latest best of breed antivirus/malware/spyware software.

17.3.8.3 Personal Computing Desktop Displays

Since desktop displays have a longer lifecycle than the computers they support, their replacement shall not be automatic at the time of a desktop replacement. Display replacement decisions for all City computers must be based on business needs, support considerations, cost-of-ownership data, and hardware compatibility considerations.

17.3.8.4 Personal Computing Processors

When establishing the minimum requirements for PC Processors and components, the I.T. Department will take in to consideration the need for the components to cost-effectively meet anticipated processing needs for the proposed productivity software, typical business needs, special needs of the mobile worker, and/or needs related to lifecycle requirements such as future availability of various memory options.

17.3.8.5 Personal Computing Optical Drives

The IT Department may not include optical drives when placing computing equipment orders. Optical Drives to read and write CDs and DVDs must be requested when there is a business need.

17.3.8.6 Lifecycle for Personal Computers

The I.T. Department shall use a lifecycle range goal of three to four years for desktop computers and three years for laptop computers.

17.3.8.7 Surge Protection and Battery Power Backup

To protect computing equipment all computers and all peripherals shall be powered through a surge protector. Computers may be powered through a battery backup power supply (UPS) for best practice.

17.3.8.9 Workstation Security

Appropriate measures must be taken when using network computers and mobile devices to ensure the confidentiality, integrity, and availability of information. The IT Department will implement security measures to include Microsoft group policies restrictions to enforce device security to protect user data and network infrastructure. All security settings will be determined and implemented by the IT Department to include but not limited to the following:

- Password protected screensaver after a period of 30 minutes of inactivity. A shorter period of inactivity may be implemented at the direction of the IT Director or the Department Head.

- Restricted access to USB ports based on an as-needed basis as determined by the IT Manager.

- Strong password policy implementation (see Password Security Policy 8:0).

- Remotely rebooting devices on a daily or as-needed basis to ensure the proper operation and integrity of the devices. **Users must close and save all open files at the end of each work shift to avoid loss of data.** The IT Department highly recommends that users reboot their PC daily at the end of their work shift to improve device performance and avoid file corruption.

17.4 Responsibilities

End-Users – Must be aware of these policies and ensure compliance.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Periodically review industry standards and update as needed.

17.5 Policy History

Adopted: 6/1/2018	Approval: City Manager

Policy 18.0 – Social Networking and Media

18.1 Purpose and Description

The City of Marco Island recognizes that Social media, professional networking sites, and personal Web sites are all useful technologies, and provide ways to build a sense of community and rapidly communicate directly to stakeholders and the general public. This policy will set forth guidelines that employees shall follow for all online communications in reference to the City of Marco Island and address the fast-changing landscape of the Internet and the way people receive their information. Social Media provides opportunities for participating departments to attract a broader audience, in addition to creating a social network allowing for residents, consumers and visitors to receive information and participate in their government in an innovative and creative way. These services are intended to enhance communications but not to diminish or circumvent existing processes. The demographic profile of the intended target audience combined with the purpose and goal of the social media initiative are the primary considerations on which to determine the appropriate use of social media. At all times, the social media initiative must align with the City's business goals and objectives.

18.2 Usage Guidelines

18.2.1 Relevant Technologies

This policy includes, but is not limited to, the following specific technologies:

- Facebook
- Snapchat
- Instagram
- LinkedIn
- Tumblr
- Twitter
- Personal Web Sites
- Personal Blogs

City of Marco Island employees are encouraged to use the following guidelines in social networking practices:

- Be relevant to your area of expertise
- Do not be anonymous
- Maintain professionalism, honesty, and respect
- Apply a "good judgment" test for every activity related to the City of Marco Island: Could you be guilty of leaking information, customer data, or upcoming announcements? Is it negative commentary regarding the City of Marco Island? Activity showing good judgment would include statements of fact about the City of Marco Island and its services, facts about already-public information, or information on the City's official website. Further, if any employee becomes aware of social networking activity that would be deemed distasteful or fail the good judgment test, please contact the Human Resources Department.

18.2.3 City of Marco Island Assets

The use of City of Marco Island assets (computers, Internet access, email, etc.) is intended for purposes relevant to the responsibilities assigned to each employee. Social networking sites are not deemed a requirement for most positions. For those employees that are permitted to access these services, a reasonable and limited amount of use of company assets are permitted for social networking services.

18.2.4 Inaccurate or Defamatory Content

Employees who participate in online communication deemed not to be in the best interest of the City of Marco Island will be subject to disciplinary action. This online communication can include but is not limited to the following:

- City information or data leakage
- Inaccurate, distasteful, or defamatory commentary about the City
- Racial slurs, sexual content, or discriminatory content

Disciplinary action can include termination or other intervention deemed appropriate by Human Resources.

18.2.5 Off-Limits Material

This policy sets forth the following items which are deemed off-limits for social networking:

- Intellectual property (data and/or software programs)
- Customer Data

The City of Marco Island's intellectual property and customer data are strictly forbidden from any online discourse except when specifically authorized by the City Manager, City Attorney and/or City Clerk.

Accessing games, sponsored content, and advertising content on social networking sites is strictly prohibited. Such activity has high potential for introducing malware and spyware on the City networked computers.

18.2.6 Sensitive Matters

Any online communication regarding proprietary information, such as layoffs, strategic decisions, or other announcements deemed inappropriate for uncoordinated public exchange is not permitted unless specific permission has been granted by the employee's Department Head. State of Florida Public Records laws and Federal Copyright laws must be strictly adhered to.

18.3 Personal Usage

City employees are discouraged from personal use of social networking via the City's Internet, mobile devices, cellular devices, and other computing systems. Such activity has high potential for misrepresentation, misconception or confusion of an individual's personal beliefs, ideals, and posts with those that represent official city related content, posts, etc.

18.4 Expectations of Online City Authorized Spokespeople

Just as with traditional media, we have an opportunity, and a responsibility, to effectively manage the City's reputation online and to selectively engage and participate in the online conversations every day. The following principles guide how an authorized City Online Spokesperson(s) should represent the City in an online, official capacity, when they are speaking "on behalf of the City of Marco Island":

1. Code of Conduct and Other Policies: Follow the City's Code of Conduct and all other City policies. As an official representative of the City, you must act with honesty and integrity in all matters. This commitment is true for all forms of social media. In addition, several other policies may govern your behavior as an authorized City spokesperson in the online social media space.

2. Representing the City: As a City representative, it is important that your posts convey the same positive, optimistic spirit that the City encourages for all of its communications. Be respectful of all individuals, races, religions, and cultures; how you conduct yourself in the online social media space not only reflects on you, it is a direct reflection on the City.

3. Don't Post Anonymously: You should identify yourself as an employee of the City, name, and when relevant, role at the City, as to not mislead readers or viewers. Employees should not use aliases or otherwise engage in covert activities.

4. Keep Records: It is critical that you keep records of our interactions in the online social media space and monitor the activities of those with whom we engage. Because online conversations are often fleeting and immediate, it is important for you to keep track of them when you're officially representing the City. Remember that online City statement can be held to the same legal standards as the traditional media communications. Keep records of any online dialogue pertaining to the City. The IT Department will assist with implementing an automated solution to archive communications when and where possible.

5. When in doubt, Do Not Post: Official spokespeople are personally responsible for their words and actions, wherever they are. As online spokespeople, you must ensure that your posts are completely accurate and not misleading, and that they do not reveal non-public information of the City. Exercise sound judgment and common sense, and if there is any doubt, DO NOT POST IT. In any circumstance in which you are uncertain about how to respond to a post, contact your Department Head or the City Manager.

6. Respect Copyrights: DO NOT claim authorship of something that is not yours. If you are using another party's content, make certain that they are approving of you utilizing their content, and make certain that they are credited for it in your post. Do not use the copyrights, trademarks, publicity rights, or other rights of others without the necessary permission of the rights holder(s).

7. Be responsible for your work: The City understands that employees engage in online social media activities at work for legitimate City purposes and that these activities may be helpful for City affairs. However, the City encourages all employees to exercise sound judgment and common sense to prevent online social media sites from becoming a distraction at work.

8. Remember that your local posts can have a global significance: The way that you answer an online question might be accurate in some parts of the world, but inaccurate (or even illegal) in others. Keep that "world view" in mind when you are participating in online conversations.

9. Know the Internet is permanent: Once information is published online, it is essentially part of

a permanent record, even if you "remove/delete" it later or attempt to make it anonymous. If your complete thought, along with its context, cannot be squeezed into a character-restricted space (such as Twitter), provide a link to an online space where the message can be expressed completely and accurately.

10. Drive the public to the City's website: Use the City's social media communications to drive the public to the City's website whenever possible. Use links with the social media sites to link to articles, forms, postings, etc., on the City's website.

18.5 City Sponsored Social Media Procedures

1. The City Manager or designee will approve the creation of all new social media sites, and the IT Department will establish the naming and accounts for all social media sites, to ensure the name is appropriate for the City of Marco Island as a government entity and is consistent with other department names and the City of Marco Island brand.

2. The City Manager or designee will designate staff to manage the content and security of the City's social media sites. It is important to ensure that the public's trust of the City of Marco Island's presence on social media sites is preserved and maintained. Since imitation sites may exist, the content and information must be monitored on a regular basis. Visual elements of the social media sites must be approved by the City's website master to reflect the public website brand of the City of Marco Island. This will ensure the visual consistency and creditability of the page(s).

3. Login information, including user IDs and passwords, will be created by the IT Department and are not permitted to be changed, altered, or modified. Passwords must be secure and adhere to all IT policies with regard to password protections. A user's social media password cannot be the same password used to log on to the City network.

4. Designated staff should obtain Department Head approval for any information to be posted on the City website prior to posting on the social media sites. Once information is posted on the City website, then a link can be included in the social media post. An exception will be made for disseminating immediate emergency information to the public, in which case the information can be posted on social media sites first and then posted on the City website.

5. Designated staff will be responsible for publishing, monitoring and updating their pages on all social media sites. Although departments will be responsible for maintaining their content, all staff will work together to monitor social media content based on the best practices and industry norms.

6. All City staff that use social media are responsible for complying with applicable federal, state, county, and city laws, regulations, and policies. Applicable laws include, but are not limited to, Public Records Law, Sunshine Law, records retention and records schedules laws, copyright laws, First Amendment, Privacy laws, and Information Technology policies established by the City of Marco Island.

7. Designated staff must put forth their best effort to archive all social media sites in order to adhere to the Public Records Law and records retention schedules. The City understands that the public may post a comment and then delete the comment before an archive may be made.

8. Social media sites that allow for correspondence with the public must be monitored on a daily basis by designated employees. Sites that do not allow for patron interactions must be monitored

on a weekly basis.

9. All messages must be consistent with other City of Marco Island content.

10. The frequency of messaging should be regular and without significant time lapses (at least weekly or more often), and the content should include relevant information.

11. Social media sites allowing public comment must be monitored by designated staff daily during working hours to ensure the comments meet certain criteria. Some social media sites, such as Facebook, allow instant commenting, while others, like YouTube, allow for a moderated/approved process. City-created social media forums must be structured narrowly to focus discussions on a particular interest of the City of Marco Island rather than creating a "public forum". Designated staff is only allowed to remove postings that do not meet the narrow focus of the City's media forum, including foul language.

12. Designated staff shall use only images to which the City retains the copyright or that have otherwise been authorized for use as related to the use of social media networks.

13. All social media sites that allow comments must include either a link to the following disclaimer, or the disclaimer should be published on the social media site:

"The purpose of this site is to present matters of public interest in the City of Marco Island, including its many residents, businesses, and visitors. We encourage you to submit your questions, comments, and concerns, but please note this is a moderated online discussion site and not a public forum. Once posted, the City reserves the right to delete submissions that contain vulgar language, personal attacks of any kind, or offensive comments that target or disparage any ethnic, racial, or religious group. Further, the City also reserves the right to delete content or links determined to: (i) be off topic; (ii) advocate illegal activity; (iii) promote particular services, products, or political organizations; or (iv) infringe on copyrights or trademarks. Please note that the comments expressed on this site do not reflect the opinions and position of the City government or its officers and employees. If you have any questions concerning the operation of this online moderated discussion site, please contact the City Clerk's office. E-mail addresses are public record under Florida Law and are not exempt from public records requirements. If you do not want your comments or e-mail address to be subject to being released pursuant to a public records request, do not send electronic mail or make comments to this entity. Instead, contact this office by telephone (239)389-5000 or in writing, via the United States Postal Service, Attn: City Clerk, 50 Bald Eagle Drive, Marco Island, FL 34145 ."

18.6 Security Standards

1. Accountability: Full responsibility for the City's social media presence and associated security risk in the social network will be specifically assigned in the City.

2. Content: Limit the information uploaded to the social network to the bare minimum required to meet business objectives. All content (text, photography, video, graphics and links) must be approved by the content owner. Refresh content regularly, label copyrighted content, and, where possible, include embedded copyright indicators. Scan uploaded and downloaded content for viruses and other inappropriate code.

3. Staff Use: Staff working in the social network on behalf of the City of Marco Island must abide by City policies regarding public and media relations. Staff should not place City content on personal pages. Content developed by staff for City government is a City asset and does not belong to the employee.

4. Messaging: Conversations with the social network messaging system must comply with City policies regarding harassment and offensive speech. Messages directed to customers, other employees, and citizens must comply with relevant laws and regulations (for example, disclaimers). Do not send messages that contain sensitive personal information through the system.

5. Monitoring: Monitor City content on a regular basis to detect unauthorized alterations, where possible. The using staff should monitor every time they post content to the site(s) or more often if necessary. IT staff should manually review the City's social media content on a weekly basis to identify visual and other performance problems.

18.7 Look and Feel Standards

In all possible cases, the look and feel of social networking accounts should follow the color-scheme of the City's Visual Identity Standards and Communications Style Guide. If no customization is offered, for example in applications such as Facebook, uploading a City of Marco Island Logo should suffice.

18.8 Enforcement

The I.T. Department will monitor social networking access through the use of technology tools. Violations will be reported to the Department Head of the offending employee and/or the City Manager for disciplinary action, if necessary.

18.9 Responsibilities

End-Users – Must be aware of these policies and ensure compliance.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Manage Internet Social Networking security. Monitor and report violations.

18.10 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 19.0 – Electronic Communication Logging

19.1 Policy

It is the policy of the City of Marco Island to log all electronic communications pursuant to the City of Marco Island Records Management Plan and the State of Florida public records laws.

19.2 Purpose/Description

In response to the findings of the Attorney General's Technology Team that Instant Messages, VoIP, Text, and Pin-to-Pin messages are not transitory in nature and could be retained by governments, the City shall log all electronic communications where we currently have the technology in place to capture this information, and shall retain the records in accordance with the General Records Schedules published by the State of Florida.

These electronic communication records are subject to public records requests including the various exemptions that are provided for in Chapter 119 of the Florida State Statutes. All public records requests for electronic records, whether related to communication transactions or not, should be forwarded to the City Clerk, or designee, for proper handling.

Employees are to assume there is no right to privacy for electronic communications on City communication devices.

19.3 Enforcement

Employees are expected to follow this policy. Violations of this policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

19.4 Responsibilities

End-Users – Must be aware of these policies and ensure compliance.

City Clerk – Receive and process request in accordance with Florida State Statutes and the City of Marco Island Records Management Plan. Designate fulfillment duties for the request to the appropriate department staff member if desired.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Maintain communication logs in accordance with the State of Florida Public Records laws and assist the City Clerk or designee with compiling electronic public records requests when needed.

19.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 20.0 – Cell Phone

20.1 Policy

As a productivity enhancement tool, the City encourages the business use of cellular telephones. Staff requests for City cellular telephone must be approved by the employee's Department Head.

20.2 Purpose/Description

The purpose of this policy is to clearly define the acceptable use of the City's cellular telephones and what actions are prohibited.

20.3 Ownership of the Cellular Service/Equipment

The City's cellular telephones belong to the City of Marco Island and the call logs of any cellular communications, as well as text messages, pictures, and stored files are accessible at all times by the City for business related or other purposes. Employees are to assume there is no right to privacy for cellular communications on City cell telephones and that activity on City owned cellular devices is subject to Florida Public Records laws.

Information sent or received in connection with the transaction of official city business on a personal cellular device is subject to Florida Public Records laws. Personal phones are not to be used for city business related text messaging and if you receive a business-related text, you are responsible for forwarding the text to your email for archiving.

20.4 Acceptable Use

Use of the City's cellular phones is intended for City related business. All employees are to use cellular phones as they would any other type of official City communications tools. Communications should fall within ethical guidelines and should not contain confidential information. Communication by cellular telephone is encouraged when it results in the most efficient and/or effective means of communication.

All text messaging, voicemail, and other device usage is subject to monitoring, review, and restrictions. Text message archival software (when and where available) may be used to facilitate retention of text messages for a period of time in accordance with the State of Florida General Records Schedules.

Employees are to assume there is no right to privacy for electronic communications on the City's communication devices.

At their supervisor's discretion, Incidental and occasional personal use of the City's cellular telephones may be permitted by City employees, but these communications will be treated the same as other business-related communication messages. The following are guidelines when using the City's cellular telephones for personal use:

- Personal incoming or outgoing calls must be kept to a minimum so that it does not consume more than a trivial amount of time.
- Personal incoming or outgoing calls must not interfere with an employee's work during working hours.

- Personal use of City's cellular phones is a privilege that may be monitored, restricted, or revoked at any time.

20.5 Prohibited Use

- Employees may not use the City's cellular telephones in any way that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale.
- Employees may not use the City's cellular telephones in any way that compromises the integrity of the City or its business.
- Employees may not use the City's cellular telephones in any way that compromises or violates the City's code of ethics or its employee handbook.
- Employees may not use the City's cellular telephones for excessive personal use as determined by the Department Head or their designee.
- Employees may not use the City's cellular telephones in any manner that creates an unsafe environment to the employee or to others. Safety is a priority.
- Employees must obey all state and local laws regarding use of cellular and mobile devices while driving. (No texting while driving, No handheld phone use, etc.)

20.6 Enforcement

Employees are expected to follow this policy. Violations of this policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

20.7 Responsibilities

End-Users – Must be aware of these policies and ensure compliance.

City Clerk – Receive and process request in accordance with Florida State Statutes and the City of Marco Island Records Management Plan. Designate fulfillment duties for the request to the appropriate department staff member if desired.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Monitor call usage and report suspected or known violations to the Department Head or their designee. Maintain communication logs in accordance with the State of Florida Public Records laws and assist the City Clerk or designee with compiling electronic public records requests when needed.

20.8 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 21.0 – Operating System Patch Policy

21.1 Policy

It is the policy of the City of Marco Island to provide and maintain up-to-date operating system critical and security patches on all laptops, desktops, servers, and mobile devices installed to protect the asset from known vulnerabilities.

21.2 Purpose/Description

Operating system patch management ensures confidentiality, integrity, and availability of data on our network systems. The IT Department has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms, which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

21.3 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all City employees. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and shall be dispatched to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

21.4 Responsibilities

End Users – Must be aware of these policies and ensure compliance. An employee shall apply approved patches by observing system notifications and rebooting computers when necessary.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Manage patching needs of all workstations and servers on the network, and routinely assess compliance with the patching policy.

21.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 22.0 – Public Key Infrastructure (PKI) (Encryption)

22.1 Policy

It is the policy of the City of Marco Island to provide secure electronic transfer of information through digital certificates where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

22.2 Purpose/Description

Digital certificates provide a method for allowing exchange of information securely over the Internet using the Public Key Infrastructure. Digital certificates provide identifying information, are forgery resistant, and can be verified. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.

22.3 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all City employees. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and the work order shall be dispatched to a team member to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

22.4 Responsibilities

End Users – Must be aware of these policies and ensure compliance. Upon issuance of the certificate, end-users provide a secure password separate from any other passwords, and utilize such password for remote access to network resources. Report any connectivity and/or certificate issues to the IT Department.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Manage the Public Key Infrastructure for creating, managing, distributing, using, storing, approving, and revoking digital certificates. Enforce the utilization of passwords when certificates are issued. Maintain functionality of the radius authentication server and compliance with the Public Key Infrastructure (PKI) policy.

22.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 23.0 – Bluetooth

23.1 Policy

It is the policy of the City of Marco Island to allow use of Bluetooth devices in an acceptable use scenario.

23.2 Purpose/Description

Bluetooth enabled devices enhance the user experience and are allowed for use within the City of Marco Island IT infrastructure with exceptions. Insecure Bluetooth connections can introduce a number of potential serious security issues; hence, there is a need for a minimum standard for connecting Bluetooth enabled device to ensure sufficient protection of Personally Identifiable information (PII) and confidential data.

23.3 Acceptable Use

1. No Bluetooth Device shall be deployed on City of Marco Island equipment that does not meet a minimum of Bluetooth v2.1 specification without written authorization from the IT Department. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy unless approved by the IT Department (i.e. Older versions of equipment may be grandfathered in by the IT Department).

2. When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where your PIN can be compromised. If your Bluetooth enabled equipment asks for you to enter your PIN after you have initially paired it, you must refuse the pairing request and repair your device when you are in a secure area.

3. All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth device and its paired equipment.

4. All Bluetooth devices shall use a minimum PIN length of 4 characters. A longer PIN provides more security.

5. All Bluetooth devices shall be in hidden mode (non-discoverable).

6. Only activate Bluetooth when it is needed.

7. Ensure device firmware is up-to-date.

23.4 Unauthorized Use

1. Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
2. Using City of Marco Island owned Bluetooth equipment on non-City of Marco Island owned Bluetooth enabled devices.
3. Unauthorized modification of Bluetooth devices for any purpose.

23.5 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all City employees. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and shall be dispatched to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

23.6 Responsibilities

End Users – Must be aware of these policies and ensure compliance. Bluetooth mode must be turned off when not in use. PII and/or City of Marco Island confidential or sensitive data must not be transmitted or stored on Bluetooth enabled devices. Bluetooth users must only access City of Marco Island information systems using Bluetooth device hardware, software, solutions, and connections *approved* by the IT Department. Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment. Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to the IT Department.

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Periodically review industry Bluetooth standards and update as needed. Report violations to Department Heads.

23.7 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 24.0 – Change Management

24.1 Policy

It is the policy of the City of Marco Island to provide documented change management whenever possible to ensure that information resources are protected against improper modification before, during, and after system implementation.

24.2 Purpose/Description

The City of Marco Island technology infrastructure is continuously becoming more complex, and increasingly more staff are dependent on the network, computers, and application programs to perform their daily tasks. As the interdependency between the IT Department's resources grow, the need for a strong change management policy is essential. From time to time, each element requires an outage for planed upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur with may result in upgrades, maintenance, or fine-tuning. Managing these changes is a critical part of providing a robust and valuable IT infrastructure. The purpose of the policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of information resources.

24.3 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all IT Department staff. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and the work order shall be dispatched to a team member to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

24.4 Responsibilities

Department Heads – Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Where at all possible, document all installations, upgrades, modifications, and changes, of server, networking, security hardware or software, patches, interim fixes, and Firewall changes, in the IT Department work order system.

24.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 25.0 – Network Account Management

25.1 Policy

It is the policy of the City of Marco Island to provide documented network account management to ensure that information resources are protected against improper use and modification and access is given on a least privilege, as authorized basis.

25.2 Purpose/Description

A user account is a set of credentials consisting of both a username and password that allows access to a system's resources. Management of all user accounts is essential is protecting the network resources from unauthorized access.

25.3 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all IT Department staff. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and the work order shall be dispatched to a team member to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

25.4 Responsibilities

Department Heads – Provide a written notice to the IT Department in a timely manner to document the hiring and termination of all employee for purposes of enabling and deactivating system access to network resources. Ensure enforcement of the policy through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Ensure all new user account creation and terminations have been authorized by the appropriate Department Head with approval by the Human Resources office via the submission of a completed IT Authorization form or via ticket submitted to the City's work order system. Document all new account creations, changes, and modifications, to all network and local machine user accounts via the IT Department work order system.

25.5 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 26.0 – Wireless

26.1 Policy

It is the policy of the City of Marco Island to provide wireless access for specific uses as determined by the IT Department.

26.2 Purpose/Description

The purpose of the policy is to secure and protect the information assets owned by the City of Marco Island. Wireless connectivity improves the end-user experience as it aids in accomplishing tasks and increasing productivity.

26.3 Acceptable Use

All wireless access rights must be authorized by the IT Department. All wireless infrastructure devices that connect to a City of Marco Island network, or provide access to City of Marco Island information must adhere to the following:

1. Be installed, supported, and maintained by the IT Department
2. Use approved authentication protocols and infrastructure
3. Use approved encryption protocols
4. Maintain a hardware address (MAC address) that can be registered and tracked.
5. Not interfere with wireless access deployments maintained by other support organizations.

26.4 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all IT Department staff. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and the work order shall be dispatched to a team member to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

26.5 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Obtain authorization from the IT Department for wireless access. Report any rogue wireless access devices, or any known attempts for unauthorized access via wireless access devices, to the IT Department immediately.

Department Heads – Provide a written notice to the IT Department in a timely manner to document the hiring and termination of all employee for purposes of enabling and deactivating system access to network resources. Ensure enforcement of the policy through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Verify compliance to this policy through various methods to include but not limited to periodic walk-thru, business tool reports, and auditing. Report violations to Department Head.

26.6 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 27.0 – Vendor Access

27.1 Policy

It is the policy of the City of Marco Island to provide vendor access to information resources for specific uses as determined by the IT Department.

27.2 Purpose/Description

The purpose of the policy is to establish the rules for vendor access to City of Marco Island resources and support services (A/C, UPS, etc.). The policy applies to all individuals who are responsible for the installation of new IT assets, and the operation and maintenance of existing IT assets, and who do or may allow vendor access for maintenance, monitoring, and troubleshooting purposes.

27.3 Requirements

Vendors must provide specific details of what they need access to. Vendor access accounts will be disabled except when in use for authorized maintenance or as deemed necessary by the IT Department for the proper functioning of the systems. Vendor access methods will be approved by the IT Department. Departments are prohibited from providing vendor access to network resources without authorization by the IT Department.

27.4 Enforcement

Implementation and Violations shall be noted in the IT Department's work order tracking system and the work order shall be dispatched to a team member to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

27.5 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Obtain authorization by the IT Department to provide vendor access to network resources. Report any known unauthorized vendor access to the IT Department immediately.

Department Heads – Provide a written notice to the IT Department in a timely manner to document the hiring and termination of all employees for purposes of enabling and deactivating system access to network resources. Ensure enforcement of the policy through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Verify compliance to this policy through various methods to include network monitoring, business tool reports, and auditing. Report violations to Department Head.

27.6 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 28.0 – Media Destruction

28.1 Policy

It is the policy of the City of Marco Island to properly dispose/sanitize/destroy physical and/or electronic IT related media.

28.2 Purpose/Description

The purpose of the policy is to outline the proper disposal/sanitization/destruction of IT related media (physical or electronic). These rules are in place to protect sensitive and classified information, employees, and the City of Marco Island.

28.3 Requirements

When no longer usable, hard drives, diskettes, tape cartridges, CDs, and other similar items used to process, store and/or transmit data shall be properly disposed of in accordance with measures established below:

1. Surplus through the use of electronic recycling with an approved vendor that meets industry standard certifications.
2. Physical destruction of the media resulting in 100% unreadability.

28.4 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all IT Department staff. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and the work order shall be dispatched to a team member to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

28.5 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Obtain authorization by the IT Department to dispose of network resources. Report any known unauthorized destruction to the IT Department immediately.

Department Heads – Provide a written notice to the IT Department in a timely manner to document the hiring and termination of all employees for purposes of enabling and deactivating system access to network resources. Ensure enforcement of the policy through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Verify compliance to this policy through various methods to include network monitoring, business tool reports, and auditing. Report violations to Department Head.

28.6 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 29.0 – Security Alerts & Advisories

29.1 Policy

It is the policy of the City of Marco Island to monitor and disseminate to staff security alerts and advisories as appropriate.

29.2 Purpose/Description

The purpose of the policy is to outline the procedures for monitoring and disseminating information related to security alerts and advisories to staff.

29.3 Requirements

Security alerts and advisories shall be obtained via various agencies such as US-CERT and MS-ISAC. Alerts deemed appropriate shall be disseminated to City staff.

29.4 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all IT Department staff. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and the work order shall be dispatched to a team member to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

29.5 Responsibilities

End-Users – Must be aware of these policies and ensure compliance. Must review all security alerts and advisories received.

Department Heads – Ensure enforcement of the policy through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Verify compliance to this policy through various methods to include network monitoring, business tool reports, and auditing. Report violations to Department Head.

29.6 Policy History

Adopted: 6/1/2018 Approval: City Manager

Policy 30.0 – Log Review

30.1 Policy

It is the policy of the City of Marco Island to collect and review logs relating to the information system security in accordance with various agency, local, state, and federal requirements.

30.2 Purpose/Description

Information regarding an incident may be recorded in several places, such as firewalls, routers, and application logs. Logs are generated, collected, and monitored for inappropriate activity and security breaches.

30.3 General Requirements

Logs generated by systems are to be maintained and reviewed according to various agency, local, state and federal requirements.

30.4 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all IT Department staff. Information security and internal audits may be conducted randomly to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the IT Department's work order tracking system and the work order shall be dispatched to a team member to remediate the issue. Repeated failures to follow policy will be reported to the violator's Department Head and may result in disciplinary action, if necessary.

End-Users – Must be aware of these policies and ensure compliance. Be aware that activity on the City network is monitored.

Department Heads – Ensure enforcement of the policy through disciplinary actions, if necessary, for those violating the policy.

I.T. Department – Maintain and monitor logs in compliance with various agency, state and federal requirements.

30.5 Policy History

Adopted: 6/1/2018 Approval: City Manager