



CITY OF <sup>TM</sup>  
MOUNT  
D O R A

INFORMATION TECHNOLOGY

# Policy Manual

Johnna Shamblin  
Information Technology Manager

Adopted by City Council November 4, 2008

Revised June 10, 2010

Revised October 27, 2011

Revised August 12 2014

This page left blank intentionally.

## Table of Contents

<b>Policy 1.0 - Governance Policy</b>	<b>1</b>
1.1 Policy	1
1.2 Management and Organization	1
1.3 Vision	1
1.4 Mission	1
1.5 Responsibilities	1
1.5 Responsibilities – (CONTINUED)	2
<b>Policy 2.0 - Information Technology Advisory Committee</b>	<b>3</b>
2.1 Policy	3
2.2 Mission of the Committee	3
2.3 Functions of the Committee	3
2.4 Membership	3
2.5 Meetings	3
2.6 Meeting Agenda's and Minutes	3
2.7 Policy History	4
<b>Policy 3.0 - Computer Hardware</b>	<b>5</b>
3.1 Policy	5
3.2 Purpose/Description	5
3.3 Enforcement	5
3.4 Responsibilities	5
3.5 Policy History	5
<b>Policy 4.0 - Computer Software</b>	<b>6</b>
4.1 Policy	6
4.2 Purpose/Description	6
4.3 Software Acquisition	6
4.4 Enforcement	6
4.5 Responsibilities	6
4.5 Responsibilities (CONTINUED)	7
4.6 Policy History	7
<b>Policy 5.0 - E-mail</b>	<b>8</b>
5.1 Policy	8
5.2 Purpose/Description	8
5.3 Ownership of the E-mail System	8
5.4 Acceptable Use	8
5.6 Retention of E-mail	9
5.7 Mailbox Limits	9
5.8 Enforcement	9
5.9 Responsibilities	9
5.10 Policy History	10
<b>Policy 6.0 - Internet</b>	<b>11</b>
6.1 Purpose and Description	11
6.2 Acceptable Use	11
6.3 Prohibited Use	11
6.4 Security and Blocked Access	11
6.5 Public Representation	11
6.6 Enforcement	12

6.7 Responsibilities	12
6.8 Policy History	12
<b>Policy 7.0 - Access to Computer Systems</b>	<b>13</b>
7.1 Policy	13
7.2 Purpose/Description	13
7.3 Enforcement	13
7.4 Responsibilities	13
7.5 Policy History	13
<b>Policy 8.0 - Password Security</b>	<b>14</b>
8.1 Policy	14
8.2 Purpose/Description	14
8.3 Password Expirations	14
8.4 Enforcement	14
8.5 Policy History	15
<b>Policy 9.0 – Data File Storage</b>	<b>16</b>
9.1 Policy	16
9.2 Purpose/Description	16
9.3 Enforcement	16
9.4 Responsibilities	16
9.5 Policy History	16
<b>Policy 10.0 - Public Records Request</b>	<b>17</b>
10.1 Policy	17
10.2 Purpose/Description	17
10.3 Enforcement	17
10.4 Responsibilities	17
10.5 Policy History	17
<b>Policy 11.0 - Instant Messaging/Chat</b>	<b>18</b>
11.1 Policy	18
11.2 Purpose/Description	18
11.3 Enforcement	18
11.4 Responsibilities	18
11.5 Policy History	18
<b>Policy 12.0 - Importing External Data</b>	<b>19</b>
12.1 Policy	19
12.2 Purpose/Description	19
12.3 Enforcement	19
12.4 Responsibilities	19
12.4 Responsibilities (CONTINUED)	20
12.5 Policy History	20
<b>Policy 13.0 – Digital Data Backup and Recovery</b>	<b>21</b>
13.1 Policy	21
13.2 Purpose/Description	21
13.3 Backup Audit Logs	21
13.4 Backup Tape Rotation	21
13.5 Enforcement	21
13.6 Responsibilities	21
13.7 Policy History	22

<b>Policy 14.0 – Remote/Mobile Network Access</b>	<b>23</b>
14.2 Purpose/Description	23
14.3 Enforcement	23
14.4 Responsibilities	23
14.5 Policy History	23
<b>Policy 15.0 – Voice Mail</b>	<b>24</b>
15.1 Policy	24
15.2 Purpose/Description	24
15.3 Acceptable Use	24
15.4 Prohibited Uses	24
15.4 Prohibited Uses (CONTINUED)	25
15.5 Abusive Use	25
15.6 Storage	25
15.7 Access and Retention	25
15.8 Enforcement	25
15.9 Responsibilities	25
15.9 Responsibilities (CONTINUED)	26
15.9a Policy History	26
<b>Policy 16.0 – Security Incident Response</b>	<b>27</b>
16.1 Policy	27
16.2 Purpose/Description	27
16.3 Scope	27
16.4 Leadership Role	27
16.5 Computer Security Incident Classification	27
16.5.3 Classification of Computer Security Incidents	28
16.6 Responsibilities	29
16.7 Policy History	29
<b>Policy 17.0 - Architectural Standards</b>	<b>30</b>
17.1 Policy	30
17.2 Purpose/Description	30
17.3 Hardware and Software Standards	30
17.3.1 Server Operating Systems	30
17.3.2 Desktop Client Operating Systems	30
17.3.3 Productivity Applications	30
17.3.4 Network Infrastructure	30
17.3.5 Security as a Platform Decision Factor	30
17.3.6 Remote Administration Platforms	31
17.3.7 Cabling Standards	31
17.3.8 Personal Computing	31
17.4 Responsibilities	32
17.5 Policy History	32
<b>Policy 18.0 – Social Networking and Media</b>	<b>33</b>
18.1 Purpose and Description	33
18.2 Usage Guidelines	33
18.2.1 Relevant Technologies	33
18.2.2 Topic Matter Guidelines	33
18.2.3 City of Mount Dora Assets	34

18.2.4 Inaccurate or Defamatory Content	34
18.2.5 Off-Limits Material	34
18.2.6 Online Recommendations	34
18.2.7 Sensitive Matters	34
18.3 Personal Usage	34
18.4 Expectations of Online City Authorized Spokespeople	35
18.5 City Sponsored Social Media Procedures	36
18.6 Security Standards	38
18.7 Look and Feel Standards	38
18.8 Enforcement	38
18.9 Responsibilities	38
18.10 Policy History	39
<b>Policy 19.0 – Electronic Communication Logging</b>	<b>40</b>
19.1 Policy	40
19.2 Purpose/Description	40
19.3 Enforcement	40
19.4 Responsibilities	40
19.5 Policy History	40
<b>Policy 20 – Cell Phone</b>	<b>41</b>
20.1 Policy	41
20.2 Purpose/Description	41
20.3 Ownership of the Cellular Service/Equipment	41
20.4 Acceptable Use	41
20.5 Prohibited Use	41
20.6 Enforcement	41
20.7 Responsibilities	42
20.8 Policy History	42
<b>Appendix A</b>	<b>43</b>
IT Authorization Form	44

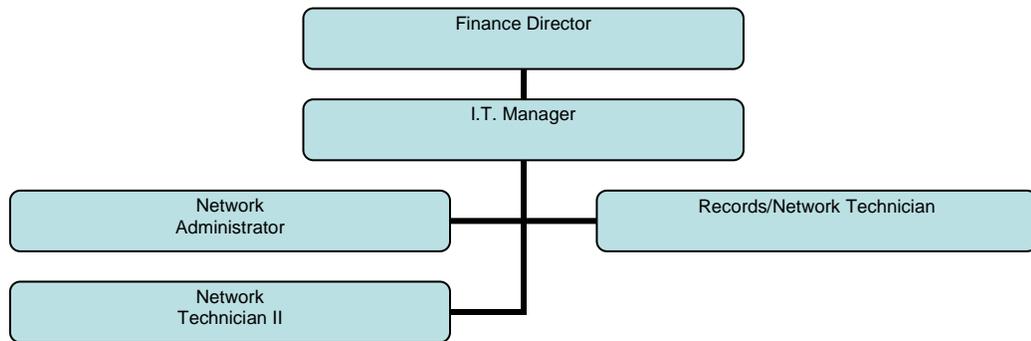
## Policy 1.0 - Governance Policy

### 1.1 Policy

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

### 1.2 Management and Organization

The Information Technology Division reports to the Finance Director.



### 1.3 Vision

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

### 1.4 Mission

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

### 1.5 Responsibilities

#### I.T. Division –

The primary responsibility of the I.T. Division 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 Mount Dora 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. Division 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, pagers, and blackberry 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. Division 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. Division staff and assists other departments in providing end-user training tailored to the needs of their staff. The I.T. Division will sponsor in-house training on applications and systems specific to the needs of our City, as well as outsource training where necessary.

Finance Director

Provide oversight to the I.T. Division

## 1.6 Policy History

Adopted: 11/04/08

Approval: City Council

Revised: 10/27/11

Approval City Manager

## **Policy 2.0 - Information Technology Advisory Committee**

### **2.1 Policy**

The City of Mount Dora 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 Division staff.

### **2.3 Functions of the Committee**

- o Make recommendations to the Information Technology Division with the purpose of increasing the effectiveness of technology and telecommunications policies and programs.
- o Provide input on current developments and future opportunities in the area of technology, e-government, and regulatory activities.
- o Advocate participation in technology and telecommunications policy formulation and implementation.
- o 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 Manager, 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 majority of the Committee. The Committee shall meet as often as necessary to complete its business. The I.T. Division 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. Division. Minutes of the meetings will be produced and forwarded to all committee members within 30 days after a meeting.

## 2.7 Policy History

Adopted: 11/04/08

Approval: City Council

Revised: 06/10/10

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. Division.

### 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. Division Manager.

### 3.3 Enforcement

The Purchasing Division will reject all requests for computer hardware that are not approved by the I.T. Division. 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 – 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.

Purchasing Division – Ensure that the I.T. Division has authorized all requests for computer hardware.

I.T. Division - 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: 11/04/08

Approval: City Council

Revised:

Approval:

## Policy 4.0 - Computer Software

### 4.1 Policy

All computer software purchased for use within the City shall be authorized and installed by the I.T. Division. 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 Mount Dora to always purchase packaged software unless there is an overwhelming business need to create a custom package. The I.T. Division 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. Division.

Acquiring software is a joint responsibility between the I.T. Division 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 Purchasing Division 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 – 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. Division 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.

Purchasing Division – Ensure that the I.T. Division has authorized all requests for computer software.

I.T. Division – 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: 11/04/08

Approval: City Council

Revised: 10/14/09

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 Mount Dora and the contents of all e-mail communication are accessible at all times by the City, with or without advance notice. Although an employee may have a personal password, the City Manager or his designee, without the employee's knowledge or consent, can access e-mail on the City's e-mail system whether business related or personal. 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

### **5.5 Prohibited Uses**

The following uses are prohibited:

- Charitable or fundraising campaigns unless specifically approved in advance by the City Manager
- Solicitations or proselytizations for commercial ventures, chain letters, religious or personal causes, or outside organizations or other similar, non job-related solicitations

## 5.5 Prohibited Uses (CONTINUED)

- o 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
- o Use of e-mail to send copies of documents in violation of copyright laws
- o Use of the e-mail system to compromise the integrity of the City or its business in any way
- o 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

The IT Department implemented an email archival system on October 1st, 2011 and imported all existing email at that time from the email server to the archival server. All incoming and outgoing email is archived on the archiving server and is searchable by the City Clerk 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, since users can search their email from the archive server instead of from their mailbox.

## 5.7 Mailbox Limits

The I.T. Division 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. Division 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. Division, when necessary.

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

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

## 5.10 Policy History

Adopted: 11/04/08

Approval: City Council

Revised: 10/27/11

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:

- o Personal usage must be kept to a minimum so that it does not consume more than a trivial amount of system resources
- o Personal usage must not interfere with an employee's productivity

### 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. Division. 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. Division as part of the original system configuration or added by IT.

### 6.4 Security and Blocked Access

The I.T. Division 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 traffic with the exception of HTTP 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. Division 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 Mount Dora may be issued unless appropriate management has granted approval.

## 6.6 Enforcement

The I.T. Division 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. Division – Manage Internet security. Monitor and report violations.

## 6.8 Policy History

Adopted: 11/04/08

Approval: City Council

Revised:

Approval

## Policy 7.0 - Access to Computer Systems

### 7.1 Policy

It is the policy of the City of Mount Dora 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. Division on Form 7-1 - I.T. Authorization Form (see Appendix A). 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. Division – 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: 11/04/08

Approval: City Council

Revised:

Approval

## 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, with the exception of providing them to the I.T. Division staff for support purposes; 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.

Passwords must meet Microsoft's complexity requirements. Passwords must be at least eight 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.

### 8.3 Password Expirations

Network logon passwords will expire on a 90-day basis and must be changed. Users may not reuse the last 24 network logon passwords.

### 8.4 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.

#### 8.5 Responsibilities

End-Users - 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. Division – Issue passwords with proper authorization and monitor compliance of the policy.

## 8.5 Policy History

Adopted: 11/04/08

Approval: City Council

Revised: 8/12/14

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.

### 9.3 Enforcement

Should the I.T. Division find City data files on an end-user’s computer, I.T. staff will assist end-users with relocating files to a network server. Continued violations of this policy will be reported to the Department Head for disciplinary action, if necessary.

### 9.4 Responsibilities

End-Users – 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. Division – Assist end-users with relocating files to network servers. Report violations to Department Heads.

### 9.5 Policy History

Adopted: 11/04/08

Approval: City Council

Revised:

Approval

## Policy 10.0 - Public Records Request

### 10.1 Policy

It is the policy of the City of Mount Dora to direct all computer system public records requests to the City Clerk pursuant to the City of Mount Dora 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 - 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 Mount Dora 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. Division – Assist City Clerk or designee with compiling electronic public records requests when needed.

### 10.5 Policy History

Adopted: 11/04/08

Approval: City Council

Revised:

Approval

## Policy 11.0 - Instant Messaging/Chat

### 11.1 Policy

Instant Messaging and all related tools (voice chat, file transfer and sharing, etc.) are prohibited on City computers, 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. Division 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 – 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. Division – 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: 11/04/08

Approval: City Council

Revised: 10/14/09

Approval: City Manager

Revised: 06/10/10

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. Division 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: floppy disk, 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. Division 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), Corel WordPerfect (.wpd), 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. Division. 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.

## **12.4 Responsibilities (CONTINUED)**

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

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

## **12.5 Policy History**

Adopted: 11/04/08

Approval: City Council

Revised:

Approval:

## Policy 13.0 – Digital Data Backup and Recovery

### 13.1 Policy

Data files maintained on the iSeries (AS/400) and network servers will be routinely backed up to electronic media for offsite storage, for the sole purpose of restoration, not preservation.

### 13.2 Purpose/Description

Information Technology will conduct backups of critical data on a Daily, Weekly, and Monthly basis. Backups will be conducted on a more frequent schedule when possible. Tape media and Disk media will be stored offsite 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. Division will maintain a log of all backup tapes within the backup software.

### 13.4 Backup Tape Rotation

Tape Backups will be performed during the night-time hours on Sunday through Friday, whenever possible. Disk Backups will be performed as frequently throughout the day as possible while limiting the impact on system performance. Backup tapes shall be rotated as follows:

- Daily tapes will be stored for at least 7 days, and no more than 30 days
- Weekly tapes will be stored for three weeks
- Monthly tapes will be stored for six months

No backup media shall be kept for more than six months. 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. Manager will periodically audit the backup logs to ensure the backups and tape rotation are properly maintained and stored off-site by I.T. staff. Continued violations of this policy will result in disciplinary action.

### 13.6 Responsibilities

End Users – Responsible for notifying the I.T. Division 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. Division – Provide for backup of network and iSeries 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: 11/04/08

Approval: City Council

Revised: 10/27/11

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 Form 14-1 I.T. Authorization Form (Appendix A). The I.T. Division 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. Division. Shall maintain physical security of remote/mobile devices and protect them from physical intrusion, theft, loss, fire, hazardous materials, flood, and other damages.

Department Heads – Provide written authorization for access rights and privileges to the I.T. Division on Form 14-1 - I.T. Authorization Form (see Appendix A). Ensure enforcement of the policies through disciplinary actions, if necessary, for those violating the policy.

I.T. Division – 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: 11/04/08

Approval: City Council

Revised:

Approval:

## 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.

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:

- o 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.
- o 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.

### 15.4 Prohibited Uses

The following uses are prohibited:

- o Charitable or fundraising campaigns unless specifically approved in advance by the City Manager
- o Solicitations or proselytizations for commercial ventures, religious or personal causes, or outside organizations or other similar, non job-related solicitations

## 15.4 Prohibited Uses (CONTINUED)

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

## 15.7 Access and Retention

End-users may access their voice mail messages through the ShoreTel Communicator 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 ShoreTel Communicator 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. Division 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

End-Users – 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.

## **15.9 Responsibilities (CONTINUED)**

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

### **15.9a Policy History**

Adopted: 11/04/08

Approval: City Council

Revised: 10/27/11

Approval: City Manager

## **Policy 16.0 – Security Incident Response**

### **16.1 Policy**

The I.T. Division will respond to computer security incidents, which may occur within the City of Mount Dora 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. Manager, and support members may include the Network Administrator, Human Resources Director, Police Chief, City Manager and 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. Manager 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. Division 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. Division 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
- 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. Division 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. Division –

- 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.
- 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: 11/04/08

Approval: City Council

Revised:

Approval:

## **Policy 17.0 - Architectural Standards**

### **17.1 Policy**

This policy establishes the City of Mount Dora's 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 Mount Dora'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. Division will continually evaluate the newest release of the Microsoft server operating systems for compatibility, functionality and business need. Upgrades will be implemented as determined feasible by the I.T. Division within the constraints of the budget and available resources.

#### **17.3.2 Desktop Client Operating Systems**

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

#### **17.3.3 Productivity Applications**

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

#### **17.3.4 Network Infrastructure**

The I.T. Division 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. Division 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. Division 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. Division 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. Division 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. Division 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**

Minimum requirements for Optical Drives shall include the ability to write CDs and read DVDs with the option to write DVDs when there is a business need.

#### **17.3.8.6 Lifecycle for Personal Computers**

The I.T. Division 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 shall be powered through a battery backup power supply (UPS) and all peripherals shall be powered through a surge protector.

## 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. Division – Periodically review industry standards and update as needed.

## 17.5 Policy History

Adopted: 11/04/08

Approval: City Council

Revised:

Approval:

## Policy 18.0 – Social Networking and Media

### 18.1 Purpose and Description

The City of Mount Dora recognizes that Social media, professional networking sites, sites, and personal Web sites are all useful technologies, and provide ways to build a sense of community as 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 Mount Dora 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:

- o Personal blogs
- o LinkedIn
- o Twitter
- o Facebook
- o MySpace
- o Personal Web Sites
- o Digg

#### 18.2.2 Topic Matter Guidelines

City of Mount Dora employees are encouraged to use the following guidelines in social networking practices:

- o Be relevant to your area of expertise
- o Do not be anonymous
- o Maintain professionalism, honesty, and respect
- o Apply a “good judgment” test for every activity related to the City of Mount Dora: Could you be guilty of leaking information, customer data, or upcoming announcements? Is it negative commentary regarding the City of Mount Dora? Activity showing good judgment would include statements of fact about the City of Mount Dora 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 Mount Dora Assets**

The use of City of Mount Dora 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 Mount Dora will be subject to disciplinary action. This online communication can include but is not limited to the following:

- o Company information or data leakage
- o Inaccurate, distasteful, or defamatory commentary about the company

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:

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

The City of Mount Dora's intellectual property and customer data are strictly forbidden from any online discourse except through mechanisms managed by Senior Management.

### **18.2.6 Online Recommendations**

Some sites, such as LinkedIn, allow members to "recommend" current or former co-workers. The City of Mount Dora employees shall not participate in employee recommendations of current or former employees for reasons of liability. All communication of this type should be referred to the Human Resources Department for verification.

### **18.2.7 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 permitted incidental and occasional personal use of social networking via the Internet. Such use will be treated the same as other business related communication.

The following are guidelines when using the City's Internet access for social networking *personal* use:

- o Personal use of social networking media as defined above must be kept to a minimum so that it does not consume more than a trivial amount of system resources
- o Personal use of social networking media as defined above must not interfere with an employee's productivity
- o 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.

## 18.4 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 Mount Dora":

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 installs in 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 possible.
5. When in doubt, Do Not Post: Official spokespersons are personally responsible for their words and actions, wherever they are. As online spokespersons, 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 Mount Dora as a government entity and is consistent with other department names and the City of Mount Dora 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 Mount Dora’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 Mount Dora. 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 must provide information to the IT Department 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 provided to the IT Department to post 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, the IT Department 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 Mount Dora.

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 the next archive is 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 Mount Dora content.

10. The frequency of messaging should be very regular and without significant time lapses (at least weekly or more often), and the content should include relevant information. Outdated 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 Mount Dora 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 Mount Dora, 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 “webmaster@ci.mount-dora.fl.us”. 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 or in writing, via the United States Postal Service, Attn: City Administration, P.O. Box 176, Mount Dora, FL 32756-0176.”

## 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 Mount Dora 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 Mount Dora Logo should suffice.

## 18.8 Enforcement

The I.T. Division will monitor social networking 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.

## 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. Division – Manage Internet Social Networking security. Monitor and report violations.

## 18.10 Policy History

Adopted: 10/14/09

Approval: City Manager

Revised: 10/26/2011

Approval City Manager

## Policy 19.0 – Electronic Communication Logging

### 19.1 Policy

It is the policy of the City of Mount Dora to log all electronic communications pursuant to the City of Mount Dora 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 Mount Dora 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. Division – 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: 06/10/10

Approval: City Manager

Revised:

Approval

## **Policy 20 – Cell Phone**

### **20.1 Policy**

As a productivity enhancement tool, the City encourages the business use of cellular telephones. Cellular telephones will be granted 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 Mount Dora and the call logs of any cellular communications, as well as text messages, 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.

### **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.

Incidental and occasional personal use of the City's cellular telephones is permitted by the 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 employees work during working hours.

### **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 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.

### **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 Mount Dora 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. Division – 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: 06/10/10

Approval: City Manager

Revised:

Approval

## **Appendix A**

## IT Authorization Form

(the form is available in a fillable .pdf format and can be submitted via email)

### CITY OF MOUNT DORA IT Authorization

Appendix A To be completed by Department Head

Form 14-1

<b>J O B I N F O</b>	Employee Name: _____	Sex: <input type="checkbox"/> Male <input type="checkbox"/> Female
	Department: _____	
	Division: _____	Employment Status:
	Primary Facility: _____ (i.e. WWTP#1, WWTP#2, WTP#1, PW Complex, Fire Station#1, etc.)	<input type="checkbox"/> NEW HIRE <input type="checkbox"/> Regular
	Job Title: _____	<input type="checkbox"/> REHIRE <input type="checkbox"/> Temporary
	Supervisor: _____	<input type="checkbox"/> CHANGE <input type="checkbox"/> FMLA
Effective Date: _____	<input type="checkbox"/> TERMINATION	

<b>E Q U I P M E N T</b>	Authorized equipment to be issued:	New equipment to be ordered:
	<input type="checkbox"/> CELL PHONE <input type="checkbox"/> New Service <input type="checkbox"/> Transfer	<input type="checkbox"/> _____
	<input type="checkbox"/> BLACKBERRY <input type="checkbox"/> New Service <input type="checkbox"/> Transfer	<input type="checkbox"/> _____
	<input type="checkbox"/> PAGER <input type="checkbox"/> New Service <input type="checkbox"/> Transfer	<input type="checkbox"/> _____
	<input type="checkbox"/> LAPTOP	<input type="checkbox"/> _____
	<input type="checkbox"/> PORTABLE PRINTER	<input type="checkbox"/> _____
COMMENTS: _____		

<b>A C C O U N T S</b>	<u>Navaline:</u>		<u>Network:</u>
	Fixed Assets <input type="checkbox"/> Add <input type="checkbox"/> Remove		Automatic rights are given to the user's own folder, the department shared folder, and the departmental applications.
	Utilities <input type="checkbox"/> Add <input type="checkbox"/> Remove		Other: _____
	Accounting (FIN only) <input type="checkbox"/> Add <input type="checkbox"/> Remove		<input type="checkbox"/> Read Only <input type="checkbox"/> Change Rights
	Payroll <input type="checkbox"/> Add <input type="checkbox"/> Remove		Other: _____
	FPO/PO Only <input type="checkbox"/> Add <input type="checkbox"/> Remove		<input type="checkbox"/> Read Only <input type="checkbox"/> Change Rights
WO/Facilities <input type="checkbox"/> Add <input type="checkbox"/> Remove			
COMMENTS: _____			

<b>T E R M I N A T I O N</b>	Termination Date: _____	<b>TO BE COMPLETED BY IT STAFF ONLY:</b>
	Equipment Returned:	Remove Network Access:
	<input type="checkbox"/> Cell Phone and Accessories Received	<input type="checkbox"/> Email Archived
	<input type="checkbox"/> Pager and Accessories Received	<input type="checkbox"/> Network Files Transferred/Archived
	<input type="checkbox"/> Laptop and Accessories Received	<input type="checkbox"/> Password Reset
		<input type="checkbox"/> Account Disabled
Comments: _____		
Employee Signature: _____	Date: _____	
Technician Signature: _____	Date: _____	

<b>A P P R O V A L</b>	Supervisor _____	Date _____
	Department Head _____	Date _____
	HR Director _____	Date _____
	IT Manager: _____	Date: _____
	Processed By: Technician: _____	Date: _____

**Property Card** (to be completed by IT Department)

Employee Name: \_\_\_\_\_ Department: \_\_\_\_\_  
 Job Title: \_\_\_\_\_ Division: \_\_\_\_\_  
 Supervisor: \_\_\_\_\_ Primary Facility: \_\_\_\_\_

Property Issued:

**CELL PHONE**     Car Charger     Wall Charger     Cases/Clips     Battery  
 Phone #: \_\_\_\_\_ Make/Model: \_\_\_\_\_ SIM: \_\_\_\_\_ S/N or /ESN(dec): \_\_\_\_\_  
 Date Issued: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_  
 Date Returned: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_  
 Cell Phone returned     Car Charger returned     Wall Charger returned     Cases/Clips returned     Battery returned

**BLACKBERRY**     Car Charger     Wall Charger     Cases/Clips     Battery  
 Phone #: \_\_\_\_\_ Make/Model: \_\_\_\_\_ SIM: \_\_\_\_\_ S/N or /ESN(dec): \_\_\_\_\_  
 Date Issued: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_  
 Date Returned: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_  
 Blackberry returned     Car Charger returned     Wall Charger returned     Cases/Clips returned     Battery returned

**PAGER**  
 Pager #: \_\_\_\_\_ Cap Code: \_\_\_\_\_ S/N: \_\_\_\_\_  
 Date Issued: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_  
 Date Returned: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_

**LAPTOP**  
 Make: \_\_\_\_\_ Model: \_\_\_\_\_ S/N: \_\_\_\_\_ IT Name: \_\_\_\_\_  
 Service Tag #: \_\_\_\_\_  
 Date Issued: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_  
 Date Returned: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_

**PORTABLE PRINTER**  
 Make: \_\_\_\_\_ Model: \_\_\_\_\_ S/N: \_\_\_\_\_ IT Name: \_\_\_\_\_  
 Date Issued: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_  
 Date Returned: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_

**OTHER**  
 Description: \_\_\_\_\_  
 Date Issued: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_  
 Date Returned: \_\_\_\_\_ Employee Signature: \_\_\_\_\_ Technician Signature: \_\_\_\_\_  
 Comments: \_\_\_\_\_