



## CITY OF WATAUGA – PERSONNEL, ADMINISTRATION AND FINANCIAL POLICIES AND PROCEDURES MANUAL

<b>POLICY TITLE</b>	<b>City Information Systems</b>
<b>INITIAL EFFECTIVE DATE</b>	<b>July 25, 2016</b>
<b>LAST REVISION DATE</b>	<b>Replaces <i>Section 27.1, 27.2, 27.3, 27.4, 27.5, 27.6, 27.7, 27.8, 27.9, 27.10 and 27.11</i> of the Personnel, Administration and Financial Policies and Procedures Manual approved on February 24, 2014.</b>
<b>POLICY NUMBER</b>	<b>14.01</b>

### **OBJECTIVE**

The City of Watauga provides computer resources or City Information Systems for the purpose of accomplishing tasks related to the City's mission. The purpose of this policy is to establish guidelines to derive the benefits of increased efficiency through the use of the City equipment, resources, use of email, internet, server and website, etc. while ensuring the protection of information assets and City integrity. The City believes the proper use of this technology saves time and money, reduces administrative overhead and improves service to the community. This policy is also enacted to preserve the integrity of the City's internal information, ensure compliance with anti-harassment and discrimination policies and prevent workplace violence and theft or misuse of City information or records.

### **SCOPE**

This policy applies to all employees and users of the City's Information System.

### **POLICY**

This policy sets forth the City's expectations and proper use of the City's Information Systems. Such systems (i.e. Internet and e-mail) are for City and business-related purposes. The use of the City Information System is a privilege, not a right. Any inappropriate use may result in cancellation of these privileges and/or disciplinary action up to and including termination. Employees are required to demonstrate responsibility and adhere to this policy when using any City Information System. Additionally, no use of the City's Information System is considered private or confidential and employees' use of those systems may be monitored by the City at any time.

All of the City's computer resources, data, networks and other communications systems and stored information which is or has been transmitted, received, or contained in the City's information Systems (including, without limitation, e-mail, Internet, pagers, voice mail, facsimiles, and information stored on computer hard drives, City thumb drives, or other data storage devices) are the City's property and are to be used solely for role-related purposes.

When using these resources, users must agree to abide by the applicable policies of the City as well as federal, state, and local laws.

## A. Definitions

1. **City Information Systems** includes hardware, software, communications networks, electronic storage media, electronic mail systems, manuals and other documentation, including those systems administered centrally or within a department, in whatever form, model, or configuration and using whatever operating systems, platforms or interfaces and whether single or multi-user, PC or network server, etc.
2. **Data** includes all files of any kind, regardless of size, format, or on what media stored or written, including but not limited to email messages, systems logs, databases, and stored information such as documents, diskettes, thumb or flash drives, etc. and commercial and locally developed software. The term also includes handwritten or printed material in paper form.
3. **Users** include employees, volunteers and any other affiliate or individual with access to use the City's computer resources. This does not include the public use of the internet through the Public Library.
4. **Provider** includes an entity that provides Internet, email, or other computer resources over a network. This term includes each personal computer owned by or leased to the City of Watauga, regardless of whether it is connected to any network system, as well as each peripheral apparatus, such as, but not limited to printers, routers, drives, wiring and cabling. The City of Watauga's Network may also provide access to other public networks and the Internet.
5. **Network** is the sum total of all computers and software owned, leased or otherwise under the control of the City, whether interconnected or not, by cables, telephone lines or other communication links.
6. **Software** is computer programs, routines and associated documentation essential to the operation and maintenance of computers.
7. **Hardware** is the physical, touchable, material parts of a computer or other electronic system.
8. **Other Communication Systems** includes telephone communication systems, pagers, postage meter, tablets, iPads, hot spots, copy machines, facsimiles, telephone service and voice mail, cell phones, workstations, printers, laptops, cameras and other related equipment used to conduct City business.

9. **Chief Information Officer** is the head of the Information Technology Department and responsible for maintaining the City's Information Systems, communicating Public Information, managing the City's social media presence and web site and providing for the daily support and training of City personnel.
10. **Virus** is a software program that is designed for the purpose of disrupting the normal operation of a computer or its software code and data.
11. **Chain mail** is any message sent to several persons requesting that each recipient send copies of the message on to any number of other persons.
12. **Junk mail** is any unsolicited e-mail consisting of mainly promotional material.
13. **Spam mail** is unsolicited and unwanted e-mail (or news postings) pushing a point generally sent to a large number of people.

## **B. Responsibilities**

1. **Information Technology Department:** The Information Technology (I.T.) Department is responsible for developing and recommending standards, procedures, policies, and guidelines to management for the purpose of meeting the needs of data integrity, security, and the maintenance of a consistent environment. The Information Technology Department is responsible for setting up employee accounts to use the Internet and e-mail as well as creating and maintaining employee I.D. cards and building security access after receiving a request from Human Resources. Information Technology must approve all downloading of non-City software from sources via the Internet. All violations uncovered through the auditing or investigations by Information Technology will be reported to the Director of Human Resources for resolution.
2. **Department Director:** The Department Director may request Internet, network, e-mail and other access for employees in their department based upon the business necessity of the department. The Department Director or designee will review and refer all requests for downloading of non-City software from the Internet to Information Technology. The Department Director should review departmental use of the Internet and e-mail. They may revoke an employee's access to such systems at any time for any misuse of the systems or violation of this policy.
3. **Director of Human Resources:** The Director of Human Resources will ensure all employees are notified of the requirements and the provisions outlined in this policy. The Director of Human Resources will conduct a prompt and thorough investigation of any violations of this policy. It is the responsibility of the Human Resources Director or designee to inform the I.T. Department of separated personnel within two (2) days prior

the planned separation date, unless unforeseen circumstances require immediate termination.

4. **Supervisor:** Every supervisor should review employee use of the City's Information Systems. They may recommend to the Department Director that an employee's access be revoked. Every supervisor is responsible for ensuring this policy is communicated and that their staff remains in compliance.
5. **Users:** All employees are responsible for adhering to the intent of this policy and following all procedures. Any employee who becomes aware of misuse or abuse of the City's Information Systems such as Internet or e-mail system must promptly contact their supervisor. If an employee mistakenly accesses restricted material, he or she must immediately notify a supervisor, the helpdesk, or the Chief Information Officer so that this material may be blocked from further access. Each employee is personally responsible for the content of their Internet and e-mail use. All employees are hereby informed that use of the City's Information Systems, Internet and e-mail is not confidential, and each employee's activities may be monitored at any time. Employees will use the Internet and e-mail system for work related matters; however, personal e-mail is permitted on a limited basis as long as such e-mail does not otherwise violate this or other applicable City or departmental policies. Employees are forewarned that all e-mail is stored and subject to the Texas Public Information Act.

It is the responsibility of the user of the email system to manage email and voicemail messages. All City related messages both sent and received from a City provided email account, must be retained in accordance with State of Texas Retention schedules. For simplicity, the City requires that all City related email messages be retained for a period of not less than 6 years. Voicemail messages however, are only required to be retained as long as they are administratively valuable and therefore may be deleted at the users' discretion. The system automatically archives email that is more than 1 year old to the users' archive folder for an additional 5 year period. However, it is the responsibility of the individual user to manage and retain any City related message in a folder within their mailbox until it meets the appropriate retention criteria.

### **C. Commitment to City Information System**

1. The City is committed to following a plan that will insure the standardization and compatibility of software, hardware, and data used for City business. By providing a consistent level of access and tools to City personnel, the City is able to improve communication and, in most cases, speed workflow.
2. The City is committed to protecting the integrity of the data it generates within its microcomputer environment from virus attacks, data corruption, system hacking by unauthorized persons, and from large unexpected disasters. Such disruptions cannot

only lead to the loss of valuable data, but also to an increase in workload for City personnel.

3. The City is further committed to providing guidelines for the use of City computers and data to insure that each is being used for the betterment of the City.
4. The City is also committed to protecting all software copyrights and to adhere to all software license agreements to which the City is a party. It is important to quantify to City personnel what is and is not considered the appropriate use of allocated equipment, system access, data, etc.
5. The City is committed to providing specific guidelines governing the functions of I.T. to insure the integrity of all data and to preserve the legal privacy of information regarding employees, citizens and business affairs in accordance with existing laws and other City policies. All data and information contained within the computer network or on City equipment is subject to the Texas Public Information Act, and may be accessible to the public under that Act upon request.
6. Virus detection software shall be installed and running at all times on each City workstation. The I.T. Department will provide monthly updates. Users must not intentionally disable the anti-virus software on their machines for any reason. If a user feels that the anti-virus software is not functioning correctly, then they should notify the I.T. Department for corrective action.
7. The I.T. Department will maintain at least a twenty-eight (28) day archive of data for the purpose of data recovery in the event data is either lost, damaged, or changed by accident or by sources outside of normal control. It shall be the responsibility of the I.T. Department to design the backup scheme and implement it. The backup method should be considered part of a disaster recovery plan.
8. The I.T. Department will not back-up users' desktops or local hard drives, and shall not be responsible for moving, maintaining or preserving any files stored in these locations.

#### **D. Prohibited Activities**

The following prohibitions are placed upon all employees of the City when using the City's Information Systems, including but not limited to City Network, Internet or e-mail. The City reserves the right to add to or modify the following list of prohibitions at any time. Any inappropriate use or failure to comply with these prohibitions may result in disciplinary action, up to and including termination.

1. Employees shall not violate copyright laws or send confidential information without prior written approval of the author, publisher, or owner.

2. Employees shall not use the internet or email to solicit for any reason that is not directly related to City business.
3. Employees shall not use the Internet or e-mail to transmit or access any material which is offensive, harassing, intimidating, disparaging, profane, obscene, sexually explicit, unethical, defamatory or threatening in nature, or which advocates an illegal act or violence or discrimination toward other people. Creating, sending or forwarding such material is grounds for disciplinary action, up to and including termination. The City has the right to block access to any site and may exercise that right at any time.
4. Employees shall not provide unauthorized access, use, alter, duplicate, destruct, or disclose any of the City's computer resources, data, including confidential or sensitive information, or proprietary information that compromises the integrity of the City and its business in any way.
5. Employees shall not hack, crack, or probe other networks or accounts.
6. Employees shall not participate in spamming, sending of unsolicited bulk mail, chain e-mail, mass postings or cross postings to news groups without prior approval from the Chief Information Officer.
7. Employees shall not be involved in any use that violates state or federal laws.
8. Employees shall not recklessly be involved in the propagation of computer worms or viruses.
9. Employees shall not be involved in the trafficking of chain e-mails or pyramid schemes.
10. Employees shall not conduct personal business or practices of any type that are intended for personal gain or misuse the systems for recreational purposes.
11. Employees shall not be involved with the illegal distribution of software otherwise known as pirating.
12. Locally installed modems or personal provider access is prohibited without the prior approval of the Chief Information Officer.
13. Employees shall not save City data to the local workstation. All sensitive and/or confidential information will be stored on the network server where access privileges can be set.
14. All employees are required to receive approval from Information Technology prior to downloading any non-city software. Employees approved for downloading software applications or executable files shall schedule these activities during the appropriate

time of day and are responsible for protecting the work environment from any virus or virus-like contamination. Every employee is required to scan all files for viruses prior to importing into City owned or leased equipment.

15. Employees are prohibited from engaging in forgery. Employees shall not misrepresent themselves or send e-mail under another employee's name, nor shall they send e-mail to anyone without identifying themselves as the sender.
16. Employees are prohibited from sharing or giving their own password, or using another employee's password or access codes.
17. Employees shall not attempt to access or read e-mail received by another employee without the authorization of the City Manager or the Director of Human Resources. Any such access will be coordinated through the Chief Information Officer.
18. Sending and receiving encrypted messages must be approved and agreed upon by the Chief Information Officer prior to sending or receiving such messages.
19. Employees receiving e-mail containing '.zip or .exe' files and other executable attachments are responsible for informing Information Technology before opening any such files.
20. Employees shall not directly email all Council Members as a group of two (2) or more members. When emailing more than one Council Member at a time, employees shall always use the "BCC" feature of the email system for inclusion of Council Member email addresses.

## **E. Privacy**

Confidential or sensitive data shall not be sent over the Internet or e-mail. Texas law requires that all employees protect the integrity of the City's confidential information as well as the confidentiality of others. Each employee is required to understand and comply with the following instructions.

1. All materials sent or received over the Internet shall be considered property of the City. An employee does not have privacy rights in any matter created, received or sent. Employees are prohibited from circumventing or blocking any privacy or security measures.
2. The City reserves the right to monitor, access or disclose any message created, received or sent via the Internet or e-mail at any time, without advanced notice.
3. Employees must comply with all other personnel policies and procedures of the City and all established departmental practices or directives. Violations discovered by

monitoring or auditing activities may be grounds for disciplinary action, up to and including termination. Additionally, illegal activity discovered may be brought to the attention of the appropriate law enforcement agency.

4. Electronic messaging systems, as well as other computer systems, are subject to the right of discovery in legal actions brought against the City.
5. Additionally, electronic messages may be subject to disclosure under the Public Information Act.

## **F. Password Security**

Any form of access or user account on any system that resides at any City facility, has access to the City network, or stores any non-public information requires user identification and system password. This form of authentication is essential in order to identify the person using an account as the authorized user and to prevent misuse by unauthorized users.

The following guidelines apply to all users (as previously defined):

1. Only the account user is allowed to login or use the computer as the user that the account is assigned to. You must not share your password with anyone under any circumstance and no individual can force you to reveal your password for any reason.
2. If misuse of computer profiles is tracked to your account, you will be assumed to have been the only person to know the password and will be held accountable for any misuse or unauthorized activity that may lead to discipline up to and including termination.
3. The Information Technology department will assign all new personnel passwords; it is incumbent upon new users to change their password at their first log on into the system.
4. Passwords should be changed every 45 days to prevent misuse or unauthorized access to your account. Passwords shall not be written down and stored in areas common to your work area where they may be easily compromised. If you believe your password has been compromised, you must change it immediately and contact the IT department.
5. Access to the City's Information Systems within the City of Watauga requires the use of an individual username and password. The username is assigned by the I.T. Department while the user sets the password. The username shall be of the following convention:
  - a. First Initial of first name + Last name
  - b. Example: The username for John Doe would be JDOE
  - c. If an identical username already exists then the scheme will take the first two initials of the first name and continue in this pattern until a unique name is created.

## **G. Access to City's Network using Personal Devices**

Only City owned workstations, laptops or portable devices may be granted access to the City's Network infrastructure. Employee owned mobile phones or tablets may also be granted access to the City's secure WiFi network on a case by case basis. The I.T. Department will not however, provide any additional user support for employee owned devices.

The voluntary use of city email accounts by an employee outside of scheduled work hours by any means shall not be considered as authorized work without prior approval by the employees' supervisor, Department Head or City Manager. Such activity will not be subject to overtime pay unless previously approved.

## **H. Purchasing Software and Hardware**

All hardware and software purchases will be coordinated through the I.T. Department. The I.T. Department will be responsible for ensuring that all software with original media is securely maintained. The I.T. Department will not be required to support any hardware or software that is purchased without prior approval.

## **I. Software Policy**

1. City of Watauga employees shall not install any software including shareware or freeware on City computers without prior authorization from the I.T. Department. Software installs are permissible on City issued tablets or phones so long as no software license agreements are in breach.
2. Employees may not duplicate any licensed or unlicensed software or related documentation purchased by the City or by other parties unless the City has established a written agreement with the Software Licensor or has purchased valid licenses.
  - a. Intentional and willful unauthorized duplication of software may subject an employee and/or the City to both civil and/or criminal penalties under the United States Copyright Act.
  - b. Intentional and willful unauthorized duplication of software shall be considered an act of serious misconduct subjecting the employee to disciplinary action.
3. City of Watauga employees may not give software to any persons outside the City (i.e. clients, contractors, and customers). Employees may use City software on the network or assigned equipment only.
4. Software and work (documents, databases, spreadsheets, etc.) developed by City employees on City equipment remain the property of the City of Watauga. Such items are for the use of the City or contractors and cannot be sold or given to anyone except in accordance with state law without consent from the department head and the I.T. Department, or by the City Manager.

5. City employees may not use City equipment and/or software during or after City hours to conduct business that is not City business. The computer systems at the City are considered City assets and should be used only for conducting City business.
6. Only licensed software may be used on City computer systems. It is the policy of the City to purchase and register all applicable licenses for all software being used on City computers. This includes shareware and freeware. If a system has shareware software installed on it, there should be a registered license on file in the I.T. library of software. There shall be no exceptions to this rule.
7. In some cases, license agreements allow for employees to use another copy of the same licensed software at home. In this case, use of City software at home will be evaluated on a case-by-case basis. Once City software is installed on a home PC, the employee remains subject to the policies of the City concerning its use, distribution, etc. Software used at home will require the approval of the department head and the I.T. Department. In addition, department heads may wish to purchase additional licenses of software for employee use at home. This will also be evaluated on a case-by-case basis.
8. The I.T. Department will maintain a register of all City software. The department will keep a library of software media, software licenses, and any documentation.
9. City computers shall not be used to play games.

#### **J. Hardware Policy**

1. City computer equipment shall not be relocated from its assigned station without the prior knowledge of and approval of the I.T. Department.
2. Unauthorized opening of the computer case; the addition of new hardware; the removal of hardware; or the otherwise modification of the computer hardware components is prohibited except where deemed appropriate by the I.T. Department.
3. Hardware upgrades will be recommended by the I.T. Department as needed. The I.T. Department may also be consulted by department heads and users as to an appropriate upgrade path for existing hardware.
4. No employee owned software is allowed to be used on City computers. Employee owned software is allowed on City issued tablets or phones so long as no software license agreements are in breach. Other peripherals, add-ons or special devices will be considered on a case by case basis.
5. All city-owned hardware directly issued to an employee shall require the employee to sign an Electronic Loan Agreement (ELA), which details all components issued to the employee. Upon separation or request from I.T., all city-owned hardware listed on the ELA shall be returned in "like" condition. Damage to, or loss of, city issued hardware by an employee shall be reviewed on a case by case basis by the I.T. Department and may subject the employee to disciplinary action or replacement charges.

6. Users shall not directly sync personal or city issued devices such as iPhones, iPads or other like devices to City computers using applications such as iTunes. City issued equipment shall be synced to the cloud only.

#### **K. Personal Folders**

1. Personal folders (Drive H) are provided to users for personal use only. City-related work shall not be stored in a user's personal folder. The content of all personal folders is subject to auditing by the I.T. Department to insure compliance with this standard. Data stored in a user's personal folder will not be backed up as part of the City's backup schedule and the City assumes no responsibility for restoring, preserving or providing copies of the files stored therein to users upon termination.
2. Users shall not save personal music or video files to their personal folder and/or to any City workstation or server. If detected, these files will be deleted and notification to the user's department head will be provided by I.T. Abuse of this policy may result in suspension of a user's network access privileges.