

# Technology and Communication Policy User Agreement

## Purpose

The purpose of Technology and Communication Policy is to provide employees, third-party contractors, consultants, and temporary employees with the acceptable usage for the City of Pueblo's technology resources. Inappropriate use of resources puts the City's network systems and services at risk from attack and/or exposes the City to legal liabilities.

## Enforcement

Employees are required to comply with the Information Technology Department (IT) Standards and Policies and to properly use the computer resources in the performance of their assigned job duties. Non-compliance with these standards and policies constitutes misuse of the City's computing resources, and may result in discipline up to and including discharge.

## Acknowledgment of these Policies

Employees are required to review and acknowledge receipt of these policies as a condition of their initial or continued employment. Once you have read these policies please sign and date this User Agreement form and return it to the HR Department.

## Policy Review Guidelines

All users, as defined in Section 1 of the Technology and Communication Policies, must read and comply with the items listed in Sections 1 thru 5. In addition:

- If you perform any of the tasks or functions listed in Table 1, you must read and comply with all items in Sections 1 thru 7.
- If you are part of the I.T. staff, you must read and comply with Sections 1 thru 9.

**Table 1**

Implement wireless connectivity	Install network telephones and or system components
Provide computer support to other users	Perform server administration
Manage or support data encryption.	Manage or support anti-virus software
Manage or support City Web sites	Purchase computers, peripheral, network, or telephone equipment.
Set or reset passwords	Install, acquire, or distribute software
Remotely access the City's network	

## Employee Acknowledgement

I affirm that I have read and understand the City of Pueblo's Technology and Communication Policies. I understand that violation of the policies or any misuse of the computer resources is grounds for discipline or discharge from employment.

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date





# **INFORMATION TECHNOLOGY**

## **Technology and Communication Policies**

**Prepared by:**  
**City of Pueblo**  
Information Technology Department  
12/29/2009  
Revision 5.0

**REVISION HISTORY**

<b>REVISION NUMBER</b>	<b>DATE</b>	<b>REASON FOR REVISION</b>	<b>REVISED BY</b>
1.0	11/30/2005	INITIAL DOCUMENT	I.T. DEPARTMENT
2.0	8/7/2006	UPDATED AND EDITED FOR WEB PUBLICATION AND EMPLOYEE MANUAL DEVELOPMENT	IT SECURITY TEAM
3.0	10/7/2008	YEARLY REVIEW	LORI PINZ
4.0	08/08/2009	YEARLY REVIEW AND UPDATE	BOBBY CUOMO LORI PINZ
5.0	12/29/2009	ATTORNEY REVIEW	TOM FLORCZAK LORI PINZ

---

**TABLE OF CONTENTS**

SECTION I – COMPUTING RESOURCE POLICY OVERVIEW .....7

    I. Purpose .....7

    II. Scope .....7

    III. Policy Definitions .....7

    IV. Ownership Policy .....7

    V. No Expectation of Privacy Policy .....8

    VI. Misuse of Computing Resources Policy .....8

    VII. Variances .....8

    VIII. Enforcement .....8

    IX. Acknowledgment of these Policies .....8

SECTION 2 - NETWORK SERVICE AND COMPUTING POLICIES .....9

    I. User Account Policy .....9

    II. User Windows Privileges .....9

    III. Remote/Home Access .....9

    IV. Software Policy .....9

    V. Anti-Virus Policy .....9

    VI. Backup Strategies and Recommendations for PCs .....10

    VII. Electronic Mail Policy .....10

    VIII. File Storage Policy .....11

    IX. Password Policy .....11

    X. Data Retention Policy .....13

    XI. Security Policy .....13

SECTION 3 – I.T. PURCHASING STANDARDS .....15

    I. Software Standard .....15

    II. Geographic Information Systems (GIS) Standards .....15

    III. PCs and Peripherals Standard .....15

SECTION 4 – I.T. SUPPORT STANDARDS .....17

    I. I.T. Computer Support Standards .....17

    II. Software Support Standards .....18

    III. Obtaining I.T. Support .....18

SECTION 5 – TELECOMMUNICATION POLICY .....19

    I. Overview .....19

    II. Personal Calls .....19

    III. Wireless Phone Service .....19

    IV. Order Processing and Service Requests .....19

    V. Long Distance Service .....19

    VI. Employee Changes or Terminations .....19

    VII. Lost or Stolen Authorization Code .....20

    VIII. Phone Features .....20

    IX. Verification of Telecommunications Charges .....20

SECTION 6 - Network Standard and Policy .....21

    I. Anti-Virus Standards .....21

    II. Routers, Switches, Hubs -Nortel Networks .....21

    III. Network transport media .....21

    IV. Encryption Policy .....21

    V. Data Standards and Policies .....22

    VI. Client Server Policy .....22

    VII. Application Development Standard and Policy .....23

    VIII. Voice System Policy .....24

    IX. Wireless Communications Policy .....24

    X. Backup and Recovery Policy .....24

    XI. Server Security Policy .....25

    XII. Software Copyrights and Licensing Policy .....26

SECTION 7 – INTRANET/INTERNET SITE POLICIES .....27

    XIII. Intranet Web-Site Policy .....27

        I. Internet Web Site Policy .....27

        II. Internetworking / Extranet Standard .....28

SECTION 8 – I.T. PROJECT REVIEW AND AWARD PROCESS .....29

    I. Overview .....29

    II. Project Review Process .....29

SECTION 9 – I.T. PROJECT MANAGEMENT PROCESS .....31

    I. Overview .....31

    II. Project Management Process .....31



## **SECTION I – COMPUTING RESOURCE POLICY OVERVIEW**

### **I. Purpose**

The purpose of these policies is to outline the acceptable use of the City of Pueblo’s technology resources. Inappropriate use of computing resources puts the City’s network systems and services at risk and exposes the City to legal liabilities.

### **II. Scope**

The policies covered in this document applies to all employees, third-party contractors, consultants, and temporary employees employed by the City of Pueblo. This policy applies to all computing and telecommunication equipment that is owned or leased by the City of Pueblo. **Please note:** If you perform any of the tasks or functions below, you are considered a power user or local administrator and are responsible for reading and complying with Sections 1- 7.

- Implement wireless connectivity
- Install network telephones and or system components
- Provide computer support to other users
- Perform server administration
- Manage or support data encryption.
- Manage or support City Web sites
- Purchase computers, peripheral, network, or telephone equipment
- Set or reset passwords
- Install, acquire, or distribute software
- Access external documents
- Remotely access the City’s network
- Manage or support anti-virus software

### **III. Policy Definitions**

**City:** Means the City of Pueblo

**City Manager:** Means the City Manager or his authorized designee

**Components:** Means pieces of equipment, i.e. hardware, software or data that alone do not form a system or provide full system functionality

**I.T.:** Means the City of Pueblo’s Information Technology Department

**Information Systems:** Means e-mail, file and application servers, desktop/laptop computers, mainframes or any piece of hardware or software used to store or transmit voice, data and/or multi-media

**Offensive materials:** Includes, but is not limited to material which is obscene, pornographic, threatening or which may be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, age, disability or religious belief

**Work product:** Includes, but is not limited to, any document, spreadsheet, compiled or composed information, program, message, e-mail, log entry, data or image

**Electronic mail (e-mail):** Means written or typed messages, such as memos or letters, sent and delivered by communications link from person to person. E-mail often consists of the primary text of the message and any attachments, such as word processing files, spreadsheet files, documents, and graphics.

**User:** Means any person who uses information systems and computer resources provided by the City of Pueblo

### **IV. Ownership Policy**

- All components, hardware or software, attached to, licensed to or installed on any City computer system or on the City’s network are the property of the City.
- The City provides computer resources, for use by its employees, for the sole purpose of conducting official City business.
- Any City employee work product, produced during City employment, whether or not it is stored on a City-owned device, becomes and remains the property of the City.

- The City, as owner of said computer systems, reserves the right of periodic examination, as it deems appropriate, of any message, data, image or software residing on or transmitted from the City's computing resources, including electronic logs and usage records.
- All servers deployed on the City of Pueblo's network must be owned and operated by the City of Pueblo's I.T. Department or approved vendor.

**V. No Expectation of Privacy Policy**

- The City and its agents, consultants and contractors, use software and information systems to monitor and record computer, phone and Internet usage for each user and is able to and does monitor or examine messages, data, or software that is on or is transmitted from its computing resources.
- Employees are not entitled to any expectation of privacy as to their usage of the City's computing or telecommunication resources including but not limited to Internet usage, e-mail and phone usage. Each employee is advised that such information is not private or confidential.
- Messages, data, or software deleted from computing resources by a user remain subject to retrieval.
- The contents of computers, phone usage and electronic mail may be subject to disclosure under the Colorado Open Records Act. This can be done by a court order or City inquiry; therefore employees are advised that much of the content of their computing systems (desktops, laptops, servers, etc.) is subject to public disclosure.
- The City reserves the right to block access from within its networks to any Internet site deemed inappropriate or which may have a detrimental effect upon network performance.

**VI. Misuse of Computing Resources Policy**

Specific conduct which will be considered misuse includes, but is not limited to, the following:

- **Excessive or Inappropriate Use:** The utilization of the Internet or any computing and telecommunication resource causing negative impact to an employee's work performance or job duties.
- **Employment:** No employee shall knowingly delete, move, hide or alter any data, documents or work product in an effort to cause delay or detriment to City business or functions when terminating employment, promoting or transferring to other City departments
- **Offensive Material:** Viewing, creating or storing offensive materials. It is a violation of policy to intentionally view, store, and print or distribute any such document or offensive graphic file unless it is directly related to the City's lawful business activities and the user's job duties.
- **Music, Video:** It is a violation of policy to download or access via the City's network any music, audio, or video content unless it is directly related to the City's lawful business activities and the user's job duties.
- **Copyrighted material:** It is a violation of policy to intentionally retrieve, view, store, or distribute material in violation of U.S. Copyright laws, including music, video, graphics, and software or data.
- **Personal Economic Gain:** The City's computing resources shall not be used in any fashion for personal economic gain including, but not limited to, private business and gambling activities.
- **The Fair Campaign Practices Act:** No employee shall engage in personal usage of City computing resources for the purpose of influencing the outcome of an election or in support of, or against, any candidate for public office or ballot issue.
- **Violation of Law:** No employee shall engage in personal usage of City computing resources in violation of any local, state or federal law, including violation of any provision of these rules and policies.

**VII. Variances**

The City Manager, Deputy City Manager or I.T. Director may grant variances to these policies.

**VIII. Enforcement**

Employees are required to comply with these Rules and Policies and to properly use the computer resources available to assist in the performance of their assigned job duties. Non-compliance with these Rules and Policies constitutes misuse of the City's computing resources and may result in discipline up to and including discharge.

**IX. Acknowledgment of these Policies**

Employees are required to review and acknowledge receipt of these policies as a condition of their initial or continued employment.

## **SECTION 2 - NETWORK SERVICE AND COMPUTING POLICIES**

### **I. User Account Policy**

- Each employee who needs access to a City of Pueblo computer must be issued a username and password specific to their specific use.
- Account information must never be shared between users and users and non-City personnel.
- Account information may be written down, but after doing so the user must treat this information in the same manner as they would treat confidential financial information. Never tape account information to your monitor, the bottom of your keyboard, or any other place that someone would be able to access the information without you being aware that they had done so.
- Usernames have a standardized form of LastnameFirstInitial (e.g. Joe Smith's username would be SmithJ). Exceptions are made only in cases where the user's standard username is already in the system or when doing so is necessary for the user to work on the system.
- Weak passwords can put the entire network at risk. IT personnel audit password complexity periodically in order to insure the security of the City's network. If your password is determined to be too weak, you will be asked to change your password. Repeated use of weak passwords may result in complexity being enforced by the City's computer systems.

### **II. User Windows Privileges**

In compliance with industry standards, the City's IT Department adheres to the principle of least possible privilege in order to minimize exposure to security risks. Any escalation of privilege must be necessitated and subsequently approved by the IT department's security administrator or IT Director.

### **III. Remote/Home Access**

- In all cases, the I.T. department must approve and setup access to the City's network or systems.
- Prolonged or multiple use access by an outside individual or agency must be approved via a formal process.
- The connecting agency is subject to the City's non-employee Extranet Agreement policies and procedures.
- Remote access for exempt City employees must be formally approved by the Director of the employee's department or the IT Director and is subject to the City's employee Extranet Agreement policies and procedures.
- Remote access for non-exempt employees is prohibited unless a variance to this policy is acquired.

### **IV. Software Policy**

- I.T. Personnel supports all software installed on City computers; however, I.T. staff may be unable to fully support the use of non-standard or specialty software.
- I.T. may decline to install, reinstall, or otherwise fix software that is not approved by the I.T. department.
- To ensure that I.T. is able to support all software installed on City computers I.T. must approve the installation and use of all software. See Section 4 for a list of supported software.
- Because all software on City computers must comply with the publishers' licensing requirements, I.T. staff will not install software unless and until ownership and proper licensing is established.
- All City employees, either temporary or full-time, must conform to copyright laws and software licensing agreements.
- Copying and/or duplicating software is prohibited unless specifically permitted within the software license agreement.

### **V. Anti-Virus Policy**

All City of Pueblo PC-based computers must have City of Pueblo's standard and supported anti-virus software installed. Any activities with the intention to create and/or distribute malicious programs into City of Pueblo's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

- The I.T. Department will install and configure virus protection software on City computers. In most cases computers on the City's LAN will be configured to automatically receive virus definition updates. It is the responsibility of

those using computers so configured to insure that recent virus protection updates are maintained and that I.T. Department staff is informed in the event of a virus infection.

- Do not open any files or macros attached to e-mail from an unknown, suspicious, or untrustworthy source. The best practice is to delete these attachments immediately, then permanently delete them by removing them from your Deleted Items folder in Outlook.
- Delete spam, chain, and other junk e-mail without forwarding.
- Do not download files from unknown or suspicious sources.
- The best practice is to avoid peer-to-peer file sharing with read/write access unless there is absolutely a business requirement to do so. Shared documents should be placed in the department's share folder (S: drive), within the intradepartmental share folder (M: drive), within the interdepartmental share folder (P: drive), or within a special share set up by I.T. Department staff.
- Always perform a virus scan on portable media (e.g. USB mass storage devices or CD-ROMs) from any unknown source before using it.

## **VI. Backup Strategies and Recommendations for PCs**

Ensuring the protection of the City's valuable information is critical. Data including but not limited to Word documents, spreadsheets, databases, presentations, and certain e-mail messages should be backed up. The ideal approach is to store data on a file server that utilizes a routine backup regimen. I.T. currently provides space, on City's servers, to each employee on the City's network. This space is normally backed up on a routine basis. To ensure that your data is safe, the following policies should be adhered to:

- Critical data should always be stored on one of the I.T. Department's file servers to insure reliable backups.
- Users are responsible for backing up any data not stored on an authorized server or mainframe, i.e. internal or external computer hard drives
- Personal files should not be stored on I.T. Department's file servers
- I.T. Department staff is not responsible for backing up or restoring personal files.

If a file is not stored on a server resource, a backup solution may not exist. Back-up alternatives are:

- CD writers (recommended)
- USB jump or thumb drives
- Tape or Zip drives

Backups should be performed on key data only. There is not a need to back up entire systems. Please contact the I.T. for back-up assistance.

## **VII. Electronic Mail Policy**

- I.T. staff shall refrain from accessing or attempting to access another individual's e-mail messages without the written permission of the user, the user's department head, I.T. Director, or City Manager.
- Treat e-mail with the same privacy and confidentiality as regular City of Pueblo mail.
- E-mail is to be considered a form of professional correspondence for the purpose of City business. Minimize the use of e-mail for personal messages.
- Target messages only to appropriate individuals. At no time should non-business related e-mail be sent to a mass distribution list. Should non-business related information need to be shared, the best mechanism for this information is the City's Intranet site. Please contact I.T. for assistance with this type of situation.
- Delete or purge unneeded or sensitive e-mail messages in a timely manner.
- Notify department head or I.T. Director of improper or undesirable use of the e-mail system. Whenever possible, a hard copy of the message should be produced. All complaints will be handled as discreetly as possible.
- All messages sent over the e-mail system fall under the Open Records Act. City of Pueblo management reserves the right to access and disclose all messages sent over its e-mail system.
- City business or correspondence conducted via e-mail must use official City e-mail addresses issued by I.T.
- Employees are not entitled to any expectation of privacy
- Obtain proper access to and documentation of e-mail by contacting the authorized network administrator.
- Use proper and professional language, which another individual would not find obscene, harassing, or profane.
- Exercise caution regarding the content of e-mail, as messages may be forwarded to persons other than the intended recipient.

- Obtain authorization from department or division management before attaching or using an Internet electronic mail system outside City of Pueblo, i.e. yahoo, hotmail, or AOL.
- Refrain from forwarding internal e-mail messages to or through e-mail systems outside City of Pueblo.
- Refrain from accessing or attempting to access another individual's e-mail messages without the permission of the e-mail owner or City of Pueblo management.
- E-mail and other information systems are not to be used in a way that may be disruptive, offensive to others, or harmful to morale. E-mail and other information systems must not be used for display or transmission of sexually explicit images, messages, or cartoons or any communication that contains ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs.
- No individual's e-mail may be monitored by anyone without prior authorization from the City of Pueblo's I.T. Director and either the City Manager or the departmental director of the individual. Such monitoring will not be authorized unless reasonable cause exists to suspect that an individual has violated a law or a City of Pueblo policy or intends to do so.

### **VIII. File Storage Policy**

- I.T. will provide space on the City's servers to store data files. Items that are stored on an employee's hard drive and NOT on a server in the provided file space may not be restorable or recoverable when the computer malfunctions.
- Data and/or e-mail stored by users who leave City employment shall be kept for up to thirty days. It will be the department's responsibility to recover that data or e-mail that is relevant and make other storage arrangements. I.T. will provide advice and assistance. After thirty days, data and e-mail will be subject to deletion by I.T.
- It is not generally recommended for users to save data to their local hard drives. Users who save to the local drive have the responsibility for devising and implementing a sound backup strategy. I.T. can assist with backup solutions in such cases.
- Shared files (files that are commonly accessed by multiple users) should only be stored on a server for which proper backup and recovery procedures have been established.
- Personal files should not be stored on I.T. Department's file servers.
- Files stored in a user's My Documents folder (or any My Documents subfolder) are stored on one of the City's file servers and are backed up regularly.
- Do not store non-work related multi-media files (e.g. MP3 or WMF) in your My Documents / My Music folder. These files take up a large amount of space and the City simply cannot accommodate the space they consume and the time they add to regular backup.
- Do not store any file that constitutes a copyright violation on City systems.
- I.T. Department staff is not responsible for backing up or restoring personal files.

### **IX. Password Policy**

- All system-level passwords (e.g., root, enable, 2000 admin, application administration accounts, etc.) must be changed on at a quarterly basis.
- All user-level passwords (e.g., e-mail, Web, desktop computer, etc.) must be changed every six months.
- All Police Department personnel passwords must meet Criminal Justice Information Systems (CJIS) standards in terms of complexity and the change interval. They are required to be changed every ninety (90) days.
- Standard users, or non-public safety, are required to change their passwords every one hundred and eighty (180) days.
- Weak passwords can put the entire network at risk. IT personnel audit password complexity periodically in order to insure the security of the City's network. If your password is determined to be too weak, you will be asked to change your password. Repeated use of weak passwords may result in complexity being enforced by the City's computer systems.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by the user.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system," and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

## i. General Password Construction Guidelines

### Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word, such as:
  - Names of family, pets, friends, coworkers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software
  - The words “City of Pueblo” or any derivation
  - Birthdays and other personal information such as addresses and phone numbers
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

### Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#%&^&\*( )\_+|~-=\`{}[]:”’<>?.,/)
- Are at least eight alphanumeric characters long
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.
- Note: Do not use either of these examples as passwords!

## ii. Password Protection Standards

- Do not use the same password for City of Pueblo accounts as for other Non-City of Pueblo access (e.g., personal Internet Service Provider accounts, option trading, benefits, etc.). When possible, don’t use the same password for various City of Pueblo access needs. For example, select one password for the computer system and a separate password for a database application system. Do not share City of Pueblo passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential City of Pueblo information.  
Here is a list of “don’ts”:
  - Don’t reveal a password over the phone to ANYONE.
  - Don’t reveal a password in an e-mail message.
  - Don’t talk about a password in front of others.
  - Don’t hint at the format of a password (e.g., “my family name”).
  - Don’t reveal a password on questionnaires or security forms.
  - Don’t share a password with family members.
  - Don’t reveal a password to coworkers while on vacation.
- If someone demands a password, refer them to this document or have them call someone in the security department.
- Do not use the “Remember Password” feature of applications (e.g., Eudora, Outlook, and Netscape Messenger).
- If an account or password is suspect of compromise, report the incident to I.T. Department and change all passwords.
- I.T. Department or department delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

## iii. Use of Passwords and Passphrases for Remote Access Users

- Access to the City of Pueblo networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.
- Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key, which is known by all, and the private key, which is known only to the user. Without the passphrase to “unlock” the private key, the user cannot gain access.

- Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against “dictionary attacks.”
- A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: “The\*?#>\*@TrafficOnThe101Was\*&!#”
- All of the rules above that apply to passwords apply to passphrases.

**X. Data Retention Policy**

- Data must be retained per the employee’s departmental standards or by the Colorado State Statutes which ever applies.
- City data, documents and work product must never be deleted when an employee terminates, promotes, or moves departments, except pursuant to authorization of the departing employee’s supervisor and Department Director, if applicable.
- Data stored on I.T. Supported devices will not be aged or deleted by the I.T. Department and will be backed up on a regular basis and will be recoverable.
- Electronic Mail backups taken by the Information Technology Department will not be retained more than two weeks.

**XI. Security Policy**

- Employees shall follow all of the security policies and procedures established by the City, for their departments and the applications they use.
- The I.T. Department reserves the right to block access from within its networks to any Internet site deemed inappropriate or which may have a detrimental effect upon network performance. Deviation from this policy requires I.T. Director approval.
- The I.T. Department manages security and sets security standards on behalf of the City for the network, servers, personal computers, computer peripherals (printers, Blackberries, palm pilots) and applicable telecommunication needs. Such management includes adoption and implementation of policies and security procedures regarding user IDs, passwords, firewalls, proxy servers, Internet practices, telecommunication and remote access to or from the City's network.
- Sponsors, administrators, and managers of specific applications are responsible for establishing the additional security policies and procedures required for use of their applications.



## **SECTION 3 – I.T. PURCHASING STANDARDS**

Users on the City’s network must use standard hardware and software supported by the I.T. Department. Request to deviate from this requires I.T. Director approval. The I.T. Department supports and will support any recommended product for the duration of its life cycle. For purchasing hardware, software, network, wireless, or peripheral items not on this list, please contact the I.T. Department.

### **I. Software Standard**

- The City’s current preferred enterprise solution is HTE or Innoprise application software whenever practical. Implementation or enhancement of enterprise software is done by I.T.
- Microsoft application software. Microsoft Office is acquired through I.T. using the volume purchase agreement. This ensures low pricing and the appropriate version of software to address the requirements. Other Microsoft application software, such as Visio, Project, Publisher and individual Office applications when needed (Word, Excel, Access, PowerPoint) will also be purchased through I.T.’s volume purchase agreement.
- Microsoft Operating Systems (Windows 7 and XP). Generally, operating system software should be purchased as part of a new PC purchase. In some cases, it is appropriate to upgrade operating systems. In such cases, the upgraded software is purchased through I.T.’s volume license.
- Software that is not the City’s property or licensed to the City should not be installed on City computers.

### **II. Geographic Information Systems (GIS) Standards**

The City of Pueblo’s Enterprise GIS system supports five departments and over thirty users. The standards listed below must be adhered to unless approval is received from the GIS coordinator. Should a user require functionality which is not available with the ESRI® software, but available with a 3<sup>rd</sup> party software approval must be received from the GIS coordinator and I.T. Department Director prior to purchasing any 3<sup>rd</sup> party software.

#### **i. GIS Desktop Standards**

- ESRI ArcGIS® product line is used for advance users performing such operations such as: spatial and data joins, geo-coding, creating shape files and building maps.
- Users must use ArcExplorer as a basic GIS tool to locate and review City information.

#### **ii. GIS Server Standards**

- MS SQL Server® is used as the relational database
- All base layers are stored on an MS SQL Server ®
- ESRI ArcSDE® is used to manipulating the GIS data within MS SQL Server ®

### **III. PCs and Peripherals Standard**

#### **iii. Desktop Computer**

- Dell Optiplex business class product lines. Minimal specifications:
  - Current Intel processor
  - Windows 7 OS
  - 120 gigabyte hard drive
  - Integrated networking & internal sound capability
  - 2 GB memory
  - 19” flat-panel monitor
  - Three-year warranty
  -

#### **iv. Notebook Computers**

- Dell Latitude minimal specifications:
  - Current Intel processor
  - Windows 7 OS
  - 80 gigabyte hard drive
  - Integrated networking & internal sound capability
  - 2 GB memory
  - 19” flat-panel monitor
  - Three-year warranty
  - Docking Station for computers on City Network

**v. Panasonic Toughbook or Dell ATG or XFR series. Minimal specifications:**

- Current Intel processor
- 80 gigabyte hard drive
- 2 GB memory
- Five-year warranty
- Backlit keyboard
- Windows 7 OS
- Integrated GOBI or wireless card
- 10.4" Touch Screen XGA
- Docking Station for computers on City Network
- 

**vi. Printers**

For specific product information and guidelines for networked, shared or stand-alone printers, contact the I.T. Department. Current printer standards utilized are below; however, I.T. department will make recommendations based on end-user requirements.

- Minolta or Canon multi-functional production units with print, copy, scan and fax capabilities
- Hewlett Packard printers are the standard if a production unit is not required.
- Warranties. 3-yr. on-site service when available.

**vii. Personal Information Managers (hand-held devices)**

Hand-held devices will be determined based on user requirements and needs. Currently, the I.T. department supports Blackberries with service provided through Verizon Wireless. The Purchasing Department is responsible for ordering and tracking of all Blackberries. I.T. is responsible for set-up and support only.

## **SECTION 4 – I.T. SUPPORT STANDARDS**

### **I. I.T. Computer Support Standards**

Supporting computer software and hardware is a responsibility that does not lend itself to being split among multiple parties. Nonetheless, I.T. recognizes the need for some computer users to regularly install and test new software on behalf of their departments. While I.T. endorses fully supporting every PC in the City, we have established these guidelines for users who would choose a degree of self-support. Placement in any of the below categories shall be at the discretion of the I.T. Director based on the best interests of the City.

#### **i. Full Computer Support**

This category is for users who just want to turn on their PC, have it work, and want I.T. to be responsible for all hardware and software problems. These PCs will be in the **pueblacity** domain. In excess of 95% of the City's PCs fit into this category. Users in this category will receive the following services:

- Ghost imaging service is available. This allows a quick restoration of a PC to working condition.
- I.T. will fully support (install, repair) all standard software.
- I.T. will provide full Outlook/Exchange service.
- I.T. will provide anti-virus software (multiple layers) and anti-spam software. This will be transparent to the user. Users may be responsible for managing their own spam filter, releasing or denying messages/senders.
- I.T. will fix any problem and replace parts at I.T.'s expense. Loaner computers will be provided as needed.
- I.T. will apply patches as needed. This will probably be done remotely and generally during off-hours.
- I.T. will provide storage on the central server (backed up by I.T.). Use is not mandatory, but recommended.

#### **ii. Limited Computer Support – City Domain**

This level of privilege is appropriate for users who must install software and are thus willing to support the PC themselves. The software in question is limited to software required to conduct City business. I.T. will base its recommendation for this level of support based on the business requirements. Including a computer or user in this category requires approval from the employee's department head and the I.T. Director. Users in this category will receive the following services:

- User staff will have local administrative rights and will be able to install software (called, for purposes of support, "user-supported software"), but not hardware (hardware installation requires full domain administrator rights that would facilitate access to any PC). If hardware frequently needs to be added/changed on a PC, it is not a good candidate for inclusion in the City's primary domain.
- I.T. will not install or reinstall user-supported software. In the event that major software or operating implementation or reinstallation is necessary, I.T. may turn over a PC at a stage of basic installation, with the user having the responsibility to complete the installation of user supported software.
- I.T. will provide storage on the central server (backed up by I.T.). Use is not mandatory, but recommended.
- Ghost imaging service is available.
- I.T. will apply patches as needed.
- I.T. must have the authority to, and will periodically audit PCs to ensure that they do not present security exposures.

#### **iii. Non-City Domain Extremely Limited Support**

This level of privilege is appropriate for users who must install software or hardware and are thus willing to support the PC. The "requirements" questions are limited to City business requirements. I.T. will base its recommendation for this level of support based on these requirements. Including a computer or user in this category requires approval from the employee's department head and the I.T. Director. Users in this category will receive the following services:

- All administrative rights are held by the user (there is no domain, thus there are no domain admin rights).
- E-mail accounts will work (i.e. jdoe@pueblo.us will still work).
- No Outlook/no Exchange will be available (requires domain membership). (Using the example above, jdoe@pueblo.us would work, but John Doe would not appear in the Outlook, and could not be scheduled for a meeting).

- No storage space on the City’s servers will be provided.
- If a PC is on the City’s network, I.T. will provide anti-virus software (multiple layers) and anti-Spam software. Signature downloads may be automatic.
- If a machine needs to be rebuilt, it is the user’s responsibility. I.T. may need to reinstall AV software. User can participate/observe all required I.T. action.
- Users with this authority must establish a strategy for keeping patches current that satisfies the City’s requirement for a secure network.
- If a computer uses the City’s network, I.T. must have the authority to, and will periodically audit the computer to ensure that it does not present security exposures.

**II. Software Support Standards**

**iv. Fully Supported Software**

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>➤ Windows 7 and XP</li> <li>➤ Internet Explorer 7 or greater</li> <li>➤ HTE Client Access software</li> <li>➤ Adobe Photoshop</li> <li>➤ ESRI ArcGIS software versions 9.2 or greater</li> <li>➤ Arcview</li> <li>➤ HighPlains Fire Safety Application</li> <li>➤ Innoprise Enterprise Application</li> <li>➤ ActiveNet Parks &amp; Recreation Application</li> </ul> | <ul style="list-style-type: none"> <li>➤ Microsoft Outlook 2000 and above</li> <li>➤ MS Office 2000 or greater</li> <li>➤ Adobe Acrobat version 5.0 or greater</li> <li>➤ Adobe Acrobat Reader</li> <li>➤ ACDSee viewer</li> <li>➤ Optiview document management and imaging system</li> <li>➤ OSSI Public Safety Application</li> <li>➤ NeoGov Applicant Tracking Application</li> <li>➤ Other applications approved by the I.T. Department.</li> </ul> |
|--|---|

**v. Unsupported or Limited Support Software**

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>➤ AutoCAD</li> <li>➤ Synchro</li> <li>➤ Highway Capacity</li> <li>➤ Jamar</li> <li>➤ HDM</li> <li>➤ Macromedia Flash</li> </ul> | <ul style="list-style-type: none"> <li>➤ Translink</li> <li>➤ TGEN</li> <li>➤ CarteGraph</li> <li>➤ Intersection Magic</li> <li>➤ Apple QuickTime viewer</li> <li>➤ Paint Shop Pro 7.0</li> </ul> |
|--|---|

**III. Obtaining I.T. Support**

- If you have questions regarding your computer or the City’s phone system, please contact the Helpdesk at ext.2400 or at 553-2400. Or,
  - Open your browser, got to <http://city/helpdesk/default.htm> and open a ticket.
  - Each work order is assigned a priority based upon the immediacy of the user’s needs. Please be sure to make IT aware of any special considerations regarding the timeliness of the response that you require.

## **SECTION 5 – TELECOMMUNICATION POLICY**

### **I. Overview**

The City provides employees with both local and long distance telephone service through the City's PBX (Private Branch Exchange) system or, as determined by needs, other telecommunications companies. City telephones are intended for City business only and include emergency calls and calls that are in the best interest of the City.

### **II. Personal Calls**

Although personal calls may be permitted during working hours, it must be of reasonable duration and frequency, and it must be: (1) a local call; (2) charged to a personal credit card; (3) charged to a home telephone; (4) charged to the called party, or (5) made to a toll free number. For any use of City telephones beyond the parameters of this policy, employees must pay the cost associated with the calls. Personal phone calls are allowed at the department head or supervisor's discretion.

Employees ARE NOT permitted to open any personal telephone accounts using their office phone number as a bill to address. Should this happen, the employee will be liable for any charges billed to the City, and the account will be canceled.

### **III. Wireless Phone Service**

Wireless phones, Blackberries, and paging services are handled through the Purchasing Department. The IT Department does not provide technical support for these services with the exception of Blackberry support.

### **IV. Order Processing and Service Requests**

The I.T. Department is responsible for ordering, tracking, installing network circuits, phone lines, and supporting the City's local and long distance phone and network needs. This includes modem, fax, extension, alarm lines and network connectivity.

NOTE: The requesting department may be responsible for paying any charges related to their requests. IT will alert the department of charges prior to authorizing work. Should a department contract services outside the IT organization, and the IT organization does not have record of these services, those services may be subject to disconnect without notification by the I.T. Department. Contracting services outside of the I.T. Department may cause our phone system warranty to be void.

### **V. Long Distance Service**

Long-distance phone service is provided to an employee through the use of a unique Forced Authorization Code (or FAC). This four-digit number is yours for your entire employment with the City. It is extremely important that you DO NOT give this code to anyone, as you are responsible for all calls made with your code. If you receive a telephone statement that contains questionable charges, you should notify I.T. This will allow your FAC to be canceled and a new one issued. The I.T. Department will investigate the suspicious calls and contact the long distance company to get a credit issued if appropriate.

Long distance charges on the bill are billed directly to our FAC, regardless of the telephone extension from which the call was placed. This feature eliminates any confusion about the person or department responsible for the calls.

### **VI. Employee Changes or Terminations**

**New Employees** – The I.T. Department will need to be contacted to obtain a FAC for all new employees. The department head or the individual in the department responsible for new employee technology requests must submit this request.

**Departmental/Termination Changes** - Should a person change departments or terminate employment with the City, I.T. will need to be contacted so that the person's FAC can be moved to their new department for billing or deactivated. The I.T. Department should be informed as soon as reasonably possible. Should a department fail to notify I.T., the department will be responsible for any charges incurred after the move/termination date or until the FAC billing has been moved to the new department unless other arrangements have been made.

**VII. Lost or Stolen Authorization Code**

Individual Departments are responsible for all charges incurred through the use of their employees Authorization Code. In the event a code is lost or stolen, you must report it immediately to the I.T. Department.

**VIII. Phone Features**

In general, the following features have been blocked by the City's PBX system.

- Collect or Third Party Calls
- 900 Type Calls
- 411 or Directory Assistance Calls
- International Calling

If your department has a need to receive or make such calls, special arrangements must be made with I.T. Department to remove this block from the system.

**IX. Verification of Telecommunications Charges**

It is the responsibility of each department to verify the accuracy of all charges and note any discrepancies or unacceptable use. A copy of all telecommunication bills can be obtained monthly from the Finance Department. If you receive a telephone statement that contains questionable charges, you should notify the I.T. Department.

## **SECTION 6 - Network Standard and Policy**

Network equipment is used to provide, manage, or optimize network traffic or services, or used to remotely access the City's network have implications for all other users on the network. As such, network strategies, network equipment and software selection, and network implementation is in the control of the I.T. Department and is subject to applicable procurement requirements.

### **I. Anti-Virus Standards**

- Responsible I.T. staff must keep virus patterns up to date either: (1) through central management or (2) in the event that centralized management is not feasible, I.T. staff will configure the computer to download virus pattern updates directly from the anti-virus vendor.
- When virus/malware infestations are discovered, I.T. staff will examine infected computers and attempt to remove the viruses/malware. If a cursory virus removal attempt fails, virus-infected computers must be removed from the network until they are verified as virus-free.
- I.T. is responsible for creating procedures that ensure that anti-virus software is run at regular intervals and that computers are verified as virus-free.
- The I.T. Department staff will monitor the virus protection status of all computers so configured. Computers that are not so configured will be configured to receive virus definition updates directly from the anti-virus vendor.

### **II. Routers, Switches, Hubs -Nortel Networks**

- Nortel Networks is the City's preferred manufacturer for most networking equipment. As the network expands, continued implementation of the Nortel architecture will facilitate a single, converged network.
- All core and critical network nodes are attached to a UPS unit.
- When practical, replacement equipment for core and critical network nodes are kept onsite.
- When it is not practical to keep replacement equipment for core and critical network nodes onsite, a replacement agreement (having an acceptable replacement time) with a third-party vendor is acceptable.

### **III. Network transport media**

- Sites on the City's network will be connected using either the City's fiber optic cable or leased T-1 circuits.
- Wireless users connect using Verizon, Edge, 1xrtt, or EV-DO for Wide Area Networking (WAN) or 802.11g (preferred) or 802.11b methodologies for local connectivity (LAN). 802.11f and b can only be used in conjunction with encrypted VPN client-server architecture.
- Remote usage via the Internet is approved on a case-by-case basis by the I.T. Department. Connection is via GoToMyPC or City VPN services.
- All data traffic on the City's network is TCP/IP.
- Network segments are within one of the following categories:
  - Ethernet Fiber optic segments, at either 10Gbps, 1Gbps, 10Mbps, 100Mbps, or T-1 speed (1.544Mbps)
  - Ethernet CAT5, CAT5E or CAT6 segments, at 10Mbps or 100Mbps
  - Leased T-1 circuit, running at 1.544Mbps

### **IV. Encryption Policy**

- Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application.
- Symmetric cryptosystem<sup>1</sup> key lengths must be at least 128 bits (256 bits for public safety transmissions over an unsecured network).
- Asymmetric cryptosystem<sup>2</sup> keys must be of a length that yields equivalent strength.
- The City of Pueblo's key length requirements will be reviewed annually and upgraded as technology allows.

<sup>1</sup> Symmetric Cryptosystem: A method of encryption in which the same key is used for both encryption and decryption of the data.

<sup>2</sup> Asymmetric Cryptosystem: A method of encryption in which two different keys are use: one for encrypting and one for decrypting the data (e.g., public-key encryption).

- The use of proprietary encryption<sup>3</sup> algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by security administration. The U.S. government restricts the export of encryption technologies.
- 128-bit encryption is required for remote connections. This connection is established using GoToMyPC or City's VPN.
- 256-bit encryption is required for wireless connections. This is required for all Public Safety and non-public safety individuals with dedicated wireless cards.
- 128-bit encryption is required for Non-Public Safety wireless or Ethernet connection accessing the network with loaner computers, i.e. notebooks given to individuals traveling.

## V. Data Standards and Policies

### i. **Data Platforms**

The Information Technology Department supports storage and use of the following platforms for the City's data:

- IBM iSeries (AS/400) for corporate data processed by HTE software
- File servers provide centrally by I.T. Department
- Databases residing on Microsoft SQL servers
- GIS data residing on the County's ESRI/MS SQL database
- Internal Web material residing on the City's Microsoft Internet Information Server

### ii. **Geographic Information Systems**

A generic map template is used for all maps produced by the GIS group within the I.T. department when at all possible. Sometimes due to the data being represented some modification must be made to location of template components, but never are any of the components removed.

#### ➤ **GIS Data and Metadata**

- All base data is available within the ESRI ArcSDE® geodatabase. Users will create subsets of data for unique projects.
- Metadata contains the information related to the construction of the data. Name, department, and purpose of the data are the minimum requirements for the metadata content.
- Metadata standards are required to be followed when data in the geo-database is utilized.
- Subsets of geodatabase data for use in projects do necessarily need to follow the minimum Metadata standards; however, the GIS Coordinator has control over determining whether or not data is required to follow these standards

#### ➤ **Geodatabase Standards**

Data will be stored in the geodatabase within the 4 categories below. Should data need to be stored outside of these 4 categories, the user must contact the GIS coordinator for approval and assistance in creating the new category.

- Geography
- Description: anything not manmade, i.e. trees, water, soils, topography
- Infrastructure
- Description: building footprints, address points, utility lines, etc.
- Government
- Description: city limit, zoning, school districts, etc.
- Transportation
- Description: roads, bus routes, trails etc.

## VI. Client Server Policy

The City of Pueblo utilizes a two-tier client server system environment for in-house developed applications. Processing and presentation occur at the end user PC level with shared production data storage on a dedicated hardware platform. The data server software of choice is Microsoft SQL Server ®. Older applications may utilize MS Access Jet Engine databases, which will eventually be migrated to SQL Server 2005®. Many of the applications also access HTE® data (in

<sup>3</sup> Proprietary Encryption: An algorithm that has not been made public and/ or has not withstood public scrutiny. The developer of the algorithm could be a vendor, and individual, or the government.

read-only mode located) located on the IBM AS/400's running 3rd party HTE® applications. The standards below must be followed for in-house developed applications.

## **VII. Application Development Standard and Policy**

Application developers must ensure their programs contain the following security precautions. Applications should:

- Support authentication of individual users, not groups.  
Not store passwords in clear text or in any easily reversible form.
- Provide for some sort of role management, so that one user can take over the functions of another without having to know the other's password.
- Support TACACS+, RADIUS, and/or X.509 with LDAP security retrieval, wherever possible.

### **iii. Development Tools**

Applications will:

- Be developed with MS Access® or other I.T. approved computer language such as Visual Basic®.
- Contain program logic, queries, macros, forms, reports etc separate from production data.
- Utilize linked data tables stored in native MS Access Jet Engine® and/or preferably, Microsoft SQL Server® databases for shared dynamic data. Static tables may be stored within the application module to enhance system performance.
- Utilize ODBC connections to SQL Server® databases limiting application access via a common User Name and Password known only to authorized IT Developers and the SQL Server® database administrator.
- Utilize Microsoft® standard security features to govern access to application system modules and data.
- Conform to a standard 'look and feel' by utilizing application templates that have been developed for uniform background appearance, button names, headings, screen navigation, application security and other components.
- Run in production from a shared executable module located in a designated shared server folder. Exception: PCs not connected to the optical fiber network may utilize a standalone version of the executable to enhance response times.

### **iv. Source Code**

- Source code for application front-end modules for development and production will be:
- Stored in I.T. server folders with standard mapped drive designations.
- Backed up according to predetermined schedules.
- Restricted to use by authorized I.T. personnel.

### **v. Executable Code**

Production application modules, objects and/or executables will be constructed, stored, secured and backed up, using a methodology that will:

- Prevent unauthorized access to raw data tables, query design, form design and other application objects, which would jeopardize data and system integrity.
- Prevent updating tables of 3rd party applications such as HTE by setting read-only attributes on ODBC or other connections.
- Prevent loss of data.

### **vi. Production Applications**

Production MS Access® applications will utilize standard MS Access® '.mde' modules that have been secured by VBA code and other methods to prevent unauthorized access to data tables, VBA code and other MS Access® objects.

### **vii. Documentation**

Documentation will consist of:

- Imbedded documentation such as comments in VBA code
- Entries in standard documentation interfaces such as the Description field in the MS Access® object listings.
- Electronic documents (.doc, .txt etc) stored within the application development folder.
- External printed-paper documents produced from MS Word®, MS Excel® and other standard software stored in a system developers indexed 3 ring binder library. Electronic backup to the printed documents will reside in the development folder as described in the above paragraph.
- Procedural documentation produced by the end users.

## **VIII. Voice System Policy**

- The I.T. Department must approve all telephones, telephone systems, and telephone lines.
- Nortel is the primary vendor for all voice and VoIP equipment. Nortel VoIP enabled network equipment is used on segments with VoIP traffic. Nortel 61 C and 11 C PBXs are utilized for core telecom functionality.
- Remote offices are connected using T-1 or fiber optic connections.
- VoIP is implemented when practical. Legacy network equipment is replaced with QoS enable Nortel equipment as needed.
- All telecom equipment is protected by UPS equipment.
- When practical, replacement equipment for core and critical telecommunications equipment is kept onsite. When it is not practical to keep replacement equipment for core and critical telecommunications equipment onsite, a replacement agreement (having an acceptable replacement time with a third-party vendor) is acceptable.

## **IX. Wireless Communications Policy**

- Access is prohibited to City of Pueblo networks via unsecured wireless communication mechanisms.
- Only secured wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the security department are approved for connectivity to City of Pueblo's networks. These systems must be installed by I.T. personal.
- Users are strictly prohibited from installing wireless access points that connect devices to the City's network.
- Systems must maintain point-to-point hardware encryption of at least 128 bits (256 bits for public safety transmissions).
- Systems must maintain a hardware address that can be registered and tracked, i.e., a MAC address.
- Systems must support strong user authentication 4 which checks against an external database such as TACACS+, RADIUS, or something similar.
  - 802.11 B/G access must be secured using VPN technology and encryption standards.
  - Citywide Verizon wireless access is provided to specially configured laptop computers.
  - Access control and 256-bit encryption is utilized for all Public Safety wireless traffic.
  - All wireless access points connecting to the City's network must be approved by IT.

## **X. Backup and Recovery Policy**

The I.T. Department requires that all information stored electronically in computerized form to be backed up periodically to ensure its safety in the event of a severe hardware interruption, software interruption, virus attack, or other disaster. Likewise, all operating software and application software necessary to access, recreate, or generate the information should also be backed up periodically. The frequency of backup will depend on the significance of the information and its frequency of change. The most current copy of backup media should be stored off site at a City of Pueblo authorized location. Procedures for recovery and restoration of the information should be documented.

This policy provides guidelines for procedures and responsibilities for management, system administrators, all users, and information technology (IT) services.

- Identify computerized systems that store information.
- Implement standard frequency of backup for each type of computer system or platform in use based on the significance of the information and its frequency of change. The City's preferred method is disk-to-disk backup; if disk-to-disk is not applicable for the system, then tape backup is required.
- Implement procedures for transferring a recent copy of backup media to a physically and environmentally secure off-site storage location.
- Monitor backup and recovery procedures and practices to ensure compliance with this policy.
- Identify I.T. staff responsible for ensuring successful back-ups.
- Test the backup to determine if data files and programs can be recovered.
- Routinely copy operating software, application software, and production information to backup media based on frequencies set by management. This applies to major systems (e.g., mid-range computers, local area network (LAN) or wide area network (WAN) servers, client/server database servers, special-purpose computers) in use by the organization. Back up all necessary data files and programs to recreate the operating environment.

---

<sup>4</sup> **User Authentication:** A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

- Transport or provide for the transportation and storage of current backup media at an off-site storage location. Storage location should be a sufficient distance from the data center to ensure protection. Consider the ease of access and retrieval from the off-site storage location, including blockage by debris, transportation, hours of operation, and physical and environmental controls.
- Develop and implement procedures for maintaining an inventory and tracking the location of backup media.
- When possible, maintain at least three generations of backup media in a “grandfather, father, son” format.
- Ensure that a recent copy of backup media is stored off site at all times.
- Document and implement procedures for the orderly recovery and restoration of information and its operating environment from backup media.
- Back up the printed documentation and preprinted forms necessary for recovery. Converting printed documentation and preprinted forms into electronic format and moving them into the City’s document management and imaging system is highly recommended.
- RAID 1 and RAID 5 is the preferred method of providing system redundancy.
- Ensure that backup is not continually performed on the same set of tapes. This is not applicable if using a disk-to-disk backup methodology.
- Back up on media that is compatible with the alternate computer system that will be used following a disaster, considering storage density, media type, and type of tape or disk drive
- Ensure that the following are stored at an off-site storage location:
  - Source and object code for production programs
  - Master files and transaction files necessary to recreate the current master files
  - System and program documentation
  - Operating systems, utilities, other environmental software and other vital records

**XI. Server Security Policy**

**viii. Ownership and Responsibilities**

All internal servers deployed on the City of Pueblo’s network must be owned and operated by the City of Pueblo’s I.T. Department or must be owned and operated by an operational group that is responsible for system administration that is approved of by the City of Pueblo I.T. Department to deploy the server(s). Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by security administration.

Information regarding the City of Pueblo’s servers must be documented and maintained within the I.T. Department. At a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location and a backup contact
- Hardware and operating system/version
- Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up to date.
- Configuration changes for production servers must follow the appropriate change management procedures.

**ix. General Configuration Guidelines**

- Operating system configuration should be in accordance with approved guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods, such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels (e.g., encrypted network connections using IPsec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

**x. Monitoring**

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs are kept online for a minimum of one week.
- Daily incremental tape backups will be retained for at least one month.
- Weekly full tape backups of logs will be retained for at least one month.
- Security-related events will be reported to internal audit, which will review logs and report incidents to I.T. management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host

**xi. Compliance**

- The internal I.T. audit group will manage audits. Internal audit will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

**XII. Software Copyrights and Licensing Policy**

- Ensure compliance with software license agreements by verifying that software is loaded on one computer for each license purchased.
- Review results of software compliance audits.
- Verify the removal of non-compliant software from the network and PCs.
- Establish and implement a procedure for monitoring compliance with software license agreements.
- Pursue noncompliance actions for employees refusing to discontinue illegal use of software.
- Inform employees of the provisions within software license agreements.
- Obtain software licenses and the necessary maintenance agreements.
- Retain copies of initial agreements for application software within the organization.
- Review results of software compliance audits.
- Conform to copyright laws and software licensing agreements.
- Copying and duplication of software is prohibited unless specifically permitted within the software license agreement.

## **SECTION 7 – INTRANET/INTERNET SITE POLICIES**

### **XIII. Intranet Web-Site Policy**

- The I.T. Department will provide hosting, server and administrative support for the City's primary Internet and Intranet sites.
- Each department represented on the City's internal website shall have the responsibility for ensuring that its material meets the standards set by I.T. Departments Intranet Policy.
- Each department represented on the site shall have the responsibility for ensuring that its material is current.
- The Intranet is administered by the I.T. Department.
- I.T. will enforce the Intranet Policy.
- I.T. will provide standard page layout guidelines and navigations methods for use throughout the site.
- Material on the Web site may not be used in any manner prohibited by law or disallowed by licenses, contract, copyrights, or City policy, regulations, or directives. Web pages will not contain legally restricted or confidential material.
- If the department that is providing the material for the site did not author or create the material, written permission to publish the information, graphics, or photographs on the site is required prior to placing it on the site.
- Provisions of the Fair Campaign Practices Act must not be violated; Material that could influence the outcome of an election must comply with that Act.
- Information regarding members of Council and other boards or commissions shall be limited to that which is necessary for Web site visitors to contact these individuals.
- No commercial or personal advertising of services and products are allowed on the site.
- Size limitations exist. Large files may need to be configured for downloading rather than direct viewing, in order to facilitate the most efficient browsing.
- Downloadable images shall be in GIF, JPEG, or PDF format.
- No audio or video files are allowed on the site at this time, except by specific agreement between the appropriate department head and the I.T. Director.

### **I. Internet Web Site Policy**

#### **i. Responsibilities**

- The I.T. Department will provide hosting, server and administrative support for the City's primary Internet and Intranet sites.
- The City's Web site is administered by the I.T Department.
- I.T. will enforce the City's Web Site Policy.
- I.T. will provide standard page layout guidelines and navigations methods for use throughout the site.
- Each department represented on the site shall have the responsibility for ensuring that its material meets the standards set by this policy.

#### **ii. Accessibility**

The City's Web site is designed and constructed to be accessible to people with disabilities. The City's Web site will endeavor to meet the accessibility requirements applicable to federal departmental agencies under Section 508 of the Rehabilitation Act.

#### **iii. Privacy**

- Visitor information collected by the City from the site will not be disclosed to parties outside the City, except when legally required.
- No unsolicited e-mail will be sent from the site. Visitors will not be added to emailing lists without their permission.

#### **iv. Copyright and Publishing Regulation Standards**

- Material on the Web site may not be used in any manner prohibited by law or disallowed by licenses, contract, copyrights, or City policy, regulations, or directives. Web pages will not contain legally restricted or confidential material.
- If the department that is providing the material for the site did not author or create the material, written permission to publish the information, graphics, or photographs on the site is required prior to placing it in the site.

**v. Content Standards**

- Electronic publications are subject to the same City policies regarding content as print publications.
- Pages should be grammatically correct with no spelling errors. Authors are strongly encouraged to have their pages reviewed by another party for typographical errors and similar problems.
- Provisions of the Fair Campaign Practices Act must not be violated; Material that could influence the outcome of an election must comply with that Act.
- Information regarding members of Council and other boards or commissions shall be limited to that which is necessary for Web site visitors to contact these individuals.
- No commercial or personal advertising of services and products are allowed on the site.
- Information (Web pages) for commercial or non-profit organizations is permissible if such organizations have a contractual relationship with a City Enterprise (Airport, Golf Courses, Waste Water Utility, Storm Water Utility) and a fee is not collected for this service.
- Size limitations exist. Large files may need to be configured for downloading rather than direct viewing, in order to facilitate the most efficient browsing.
- Acronyms should be used sparingly and never as a first reference.
- Downloadable images shall be in GIF, JPEG, or PDF format.
- No audio or video files are allowed on the site at this time, except by specific agreement between the appropriate department head and the I.T. Director.
- Graphics should be used sparingly, to improve the appearance of the page or to clarify its content. A “photo gallery” may be established to allow visitors who so choose to access additional graphic images.

**vi. Web Page Usage Standards**

Web sites supported by the City, either internal or external, shall be configured as follows:

- All Web publications should endeavor to meet the standards applicable to federal agencies under Section 508 of the Rehabilitation Act as amended in 1998.
- It is not necessary to provide for resolution lower than 800 X 600.
- For streaming purposes, audio and video shall be in a format compatible with Microsoft Media Player.

**vii. Web Architecture Standards**

- The City’s Web site is currently externally hosted. All components within the hosted site must comply with the LAMP architecture (Linux, Apache, MySQL, and PHP).
- It is acceptable to link to other Web servers (such as a video streaming server) that do not comply with the LAMP architecture.
- The City’s internal web site (intranet is based on Microsoft architecture, and is comprised of Microsoft’s Internet Information Server (IIS) and MS SQL.
- For users publishing to the Internet, FrontPage is the preferred publishing tool.

**viii. Links to Other Sites**

- The City’s Web site shall only link directly to pages of other public sector (government) agencies, the non-profit sector, community organizations, organizations with which the City has a professional relationship, to events which are sponsored or endorsed by such agencies or organizations or to utility companies providing service to the City of Pueblo and/or its citizens.
- The site will not link to any personal pages/sites.
- The City reserves the right to not link to any site, irrespective of whether it qualifies for linking per the guidelines in this policy.

**II. Internetworking / Extranet Standard**

- Remote usages via the Internet or Verizon wireless must utilize approved VPN technology and comply with the City’s current encryption policy.
- All connections to outside nodes must employ multiple protection layers.

## **SECTION 8 – I.T. PROJECT REVIEW AND AWARD PROCESS**

### **I. Overview**

The I.T. Project Review process provides the methodology for project identification, project benefit, vendor participation and evaluation, budget control and project award. These processes are utilized to guarantee a fair award process and a cost-effective implementation and use of tax dollars for technology throughout the City.

### **II. Project Review Process**

#### **i. Project Identification**

Project identification is the first step in the Project Review Process and is used to determine the organizational technological needs of the City. It explores the users' needs, and converts them into a formal, planned, resourced and funded project. It defines the project's objectives and goals and establishes a compelling business case for the project. It assists in acquiring commitment and approval from the appropriate level of management. The I.T. Department applies the following steps during project identification:

- Step 1: Identify projects through departmental requests
- Step 2: Discuss and determine project feasibility
- Step 3: Document applicable projects
- Step 4: Prioritize projects
- Step 5: Identify project sponsor(s)
- Step 6: Select the projects to be pursued
- Step 7: Establish objectives and goals
- Step 8: Research the technology required by the project
- Step 9: Submit estimated costs during budget process
- Step 10: Obtain executive approval and commitment
- Step 11: Prepare initial project plan and timeline
- Step 12: Determine, which bid process to utilize

#### **ii. Bid Process**

The bid process provides a consistent method for supplying vendors, wishing to acquire City business, with the project definition, objectives, and scope of work, assumptions, project deliverables and evaluation criteria. It ensures a level playing field for all vendors and establishes consistent evaluation criteria used to review vendor responses and award City business. The following steps are performed during the bid process:

- Step 1: In consultation with the Purchasing Agent, determine Bidding method:
  - RFP (Request for Proposal) – a very detailed and contractually binding document used to describe the products and/or services, the conditions under which those items are to be provided, and the relevant cost.
  - RFI (Request for Information) – a minimally detailed document used to obtain information on an intended or future purchase. It determines vendor interest and solicits a general description of available products. An RFP is then developed from the information received in the vendors' responses.
  - IFB (Invitation for Bid) – used to obtain pricing and service for a specific product or service. A contract is then awarded to the lowest bidder.
- Step 2: Identify project team members and project manager responsible for RFP, RFI or IFB creation
- Step 3: Develop vendor evaluation criteria
- Step 4: Develop RFP, RFI, or IFB
- Step 5: Obtain team approval or executive approval as needed for document
- Step 6: Submit to Purchasing for finalization and publication
- Step 7: Publish documentation
- Step 8: Publish applicable addendums
- Step 9: Identify review team
- Step 10: Hold consolidated vendor meeting if applicable
- Step 11: Receive bid information from vendors
- Step 12: Begin Award Process

**iii. Award Process**

This process provides a reliable method for evaluating vendor responses and awarding a contract for the solution that best meets the needs of the City. It ensures that the review team is objective and consistent throughout the award process, and that all vendors are evaluated fairly without bias. The following steps are performed in this process and are coordinated with and through the Purchasing Agent:

Step 1: Review vendor responses

Step 2: Score according to evaluation criteria

Step 3: Identify finalists

Step 4: Notify finalists

Step 5: Notify non-finalists

Step 6: Schedule finalists' product demonstrations, if applicable

Step 7: Conduct demonstrations with review team and stakeholders

Step 8: Critic presentations according to evaluation criteria including stakeholder feedback

Step 9: Identify award recipient

Step 10: Notify award recipient and begin contract negotiations

Step 11: Send elimination letters to remaining respondents

Step 12: Begin Project Management Phase

## **SECTION 9 – I.T. PROJECT MANAGEMENT PROCESS**

### **I. Overview**

The I.T. project management process provides the methodology utilized for project implementation, quality standards and budget control. It also provides an integrated structure for project organization, planning and management guaranteeing standards of quality and project success.

### **II. Project Management Process**

#### **i. Planning Phase**

The planning phase is executed in order to gain a mutual understanding of the project objective(s). It assists in producing a clear and explicit plan for the overall project. Items that need to be determined during this phase include project team recruitment, project deliverables, project tasks, task assignments, resources and timescales. The City's project management process consists of five phases or processes. These processes, many times, run in parallel. The following steps are performed during the planning phase:

- Step 1: Identify I.T. project manager
- Step 2: Identify project team including vendor project team
- Step 3: Complete contract negotiations
- Step 4: Finalize contracts and costs
- Step 5: Obtain executive contract and City attorney approval
- Step 6: Submit ordinance, resolution or both as required to Agenda Review Process. If Council approval is not needed, go to step 8.
- Step 7: Obtain City Council approval
- Step 8: Hold Kick-off meeting
- Step 9: Determine and document project detail
- Step 10: Develop initial project work plan and timeline
- Step 11: Determine and document project communication procedures
- Step 12: Determine and document change procedures
- Step 13: Develop and document implementation and long-term customer support processes
- Step 14: Determine post-implementation evaluation criteria/metrics
- Step 15: Determine end-user and I.T. staff training plan
- Step 16: Hold regularly scheduled project team meetings and stakeholder meetings as applicable

#### **ii. Analysis Phase**

The analysis phase takes a granular glance into the project. It provides the mechanism for the project manager to identify potential impacts, evaluate priorities, determine and allocate resources, monitor the attainment of project goals, and see where corrective action needs to be taken to keep the project on course. The City's analysis phase consists of the following steps:

- Step 1: Gather and analyze user requirements
- Step 2: Analyze proposed solution ensuring user requirements are satisfied
- Step 3: Identify risks or project exposures
- Step 4: Re-define tasks, dependencies, constraints, approach, deliverables, and resources based on risks
- Step 5: Re-define critical path based on project exposures
- Step 6: Identify end-user and I.T. staff training needs
- Step 7: Update work plan and timelines as necessary
- Step 8: Manage project scope, project changes, project/budget creep
- Step 9: Continue on-going planning activities

#### **iii. Design Phase**

The design phase provides the methodology used to create a precise solution for the project. It provides the blueprint for the detailed plans and specifications necessary to make the solution a reality. The design phase contains the following steps:

- Step 1: Layout project according to the specifications gathered during analysis
- Step 2: Finalize user requirements and detailed project specifications
- Step 3: Develop initial solution
- Step 4: Identify and manage project risks or exposures

- Step 5: Adjust design as needed to address any risks or project exposures
- Step 6: Evaluate and manage project plan, tasks, deliverables, and resources
- Step 7: Evaluate and adjust critical path
- Step 8: Evaluate and manage scope and budget creep
- Step 9: Finalize design
- Step 10: Procure project equipment
- Step 11: Develop and document test plan
- Step 12: Identify and begin pre-implementation tasks
  - o Hold pre-implementation meetings
  - o Adjust training plan and prepare training schedule
  - o Develop implementation plan
  - o Develop implementation user support plan (helpdesk numbers, contact numbers etc.)
- Step 13: Develop test plan
- Step 14: Perform testing according to test plan
- Step 15: Identify and manage problems from testing
- Step 16: Adjust design as needed to address testing issues
- Step 17: Evaluate/manage project plan, tasks, deliverables, and resources
- Step 18: Evaluate and adjust critical path
- Step 19: Approve testing
- Step 20: Prepare for implementation
- Step 21: Continue on-going planning and analysis activities

**iv. Implementation Phase**

The implementation phase brings the project to fruition. This phase consists of the following:

- Step 1: Determine if all project material has been received
- Step 2: Provide users with implementation plan
- Step 3: Begin training
- Step 4: Implement solution
- Step 5: Manage critical path and scope creep
- Step 6: Manage implementation problems
- Step 7: Adjust implementation plan as needed
- Step 8: Adjust project work plan as needed
- Step 9: Rectify all implementation issues
- Step 10: Finish Install
- Step 11: Develop post-implementation sign-off sheet
- Step 12: Schedule post-implementation team meeting
- Step 13: Sign-off on post-implementation items
- Step 14: Obtain executive sign-off for project
- Step 15: Close project or start Phase II planning
- Step 16: Submit payment to vendor for services

**v. Support Phase**

The support phase includes activities required to ensure that the end product is and continues to function and perform efficiently. It provides the tasks, equipment, skills, personnel, facilities, materials, services, supplies, and procedures required to guarantee performance and end-user satisfaction.

The following steps are used by the City's I.T. Department during this phase:

- Step 1: Solicit and obtain user feedback on implementation
- Step 2: Capture post-implementation evaluation data determined during the planning phase
- Step 3: Analyze data
- Step 4: Identify/manage post-implementation issues identified during post-implementation data analysis
- Step 5: Determine next steps for identified problems or changes
- Step 6: Monitor user problems and address accordingly
- Step 7: Utilize I.T. Helpdesk processes for future problem resolution or improvement